ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"DISEÑO DE LA RED INALÁMBRICA Y SISTEMA DE SEGURIDAD MEDIANTE CÁMARAS INALÁMBRICAS CON MONITOREO REMOTO PARA EL EDIFICIO DE LA EMPRESA METROPOLITANA DE OBRAS PÚBLICAS DE QUITO (EMOP-Q)".

CARLOS ANDRÉS AMAYA MANTILLA

Sangolquí – Ecuador

2007

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: "*Diseño de la red inalámbrica y sistema de seguridad mediante cámaras inalámbricas con monitoreo remoto para el edificio de la Empresa Metropolitana de Obras Públicas de Quito (EMOP-Q).*" ha sido desarrollado en su totalidad por el señor CARLOS ANDRÉS AMAYA MANTILLA con C.C. 171001539-5, bajo nuestra dirección.

DIRECTOR	**CODIRECTOR**
Ing. Fabián Sáenz E.	Ing. David Andrade T.

RESUMEN DEL PROYECTO

El diseño de la red inalámbrica y el sistema de seguridad inalámbrica con monitoreo remoto para el edificio de la EMOP-Q se realizó con la aplicación del estándar Wi.-Fi 802.11 desarrollado por la IEEE, el cual indica los métodos de transmisión y recepción de las ondas de radio bajo las frecuencias de 2.4 y 5 GHz y los métodos de seguridad que se aplican en las redes WLAN. Este tipo de red es un sistema flexible de comunicaciones de datos que se puede implementar como extensión o alternativa a una red LAN cableada.

Para el diseño de la red inalámbrica se realizó la selección de equipos de acuerdo a las características que presentan las marcas de productos inalámbricos más destacadas; se desarrolló también los análisis de cobertura que involucran la medición de potencia de las señales Wi-Fi de acuerdo a la estructura y distribución de puntos de trabajo del edificio para obtener una comunicación de alta velocidad. Luego de esto se realizó la configuración de los puntos de acceso que se presentan en el diseño.

Para el sistema de seguridad inalámbrica se desarrolló también un estudio de cobertura, para todo el edificio, que depende de las características de alcance de los equipos que se seleccionaron. Se configuró las cámaras inalámbricas IP así como también el software de monitoreo.

DEDICATORIA

Este proyecto lo dedico en primer lugar a mis padres por haberme apoyado en todo momento de mi vida y por brindarme su confianza y cariño incondicional. También por haberme brindado mis estudios y darme la oportunidad de surgir profesionalmente.

A mis hermanos Santiago y Daniel por que ellos son parte de mi y siempre hemos estado juntos en todo momento.

A Ibeth por brindarme su cariño, comprensión y atención siempre y por apoyarme en muchos aspectos para haber culminado con éxito este proyecto.

A toda mi familia, mis abuelos, mis tías, mis tíos que me han ayudado de una u otra forma para llegar al fin de mi carrera universitaria.

A todos mis amigos que me han brindado su amistad sincera y con los cuales hemos vivido muchos buenos momentos en nuestra vida estudiantil.

Carlos Andrés Amaya Mantilla

AGRADECIMIENTO

Agradezco a mi madre por ser un ejemplo de vida y de superación, por darme la vida, por darme su cariño.

A mi padre por todo lo su apoyo y cariño, por su confianza y su esfuerzo por darme mi educación.

A Dios por darme salud y fuerzas para luchar por mis ideales.

PRÓLOGO

El proyecto que se presenta a continuación tiene como objetivo introducirse en el ámbito de las redes inalámbricas empresariales ya que en la actualidad la tecnología inalámbrica está creciendo y desarrollándose de manera excepcional en el mercado de las redes, obteniendo así, equipos que están al alcance de cualquier empresa que requiera servicios de red.

Este proyecto envuelve temas relacionados con la tecnología inalámbrica para redes de comunicación pero se enfoca también en indicar que la tecnología inalámbrica tiene muchas aplicaciones, una de ellas son los sistemas de seguridad inalámbricos que en la actualidad es un método de seguridad muy utilizado desde usuarios caseros hasta grandes empresas. Con el fin de controlar las acciones que se realicen en su entorno.

Se trata también de dar al lector una idea del funcionamiento y de las características de los equipos inalámbricos que se utilizan al momento de diseñar redes y sistemas de seguridad inalámbricas, y también de los estándares que estos equipos utilizan, haciendo una comparación entre las marcas de productos que mas se destacan en el mundo wireless.

ÍNDICE DE CONTENIDO

CERTIFICACIÓN
RESUMEN DEL PROYETO
DEDICATORIA
AGRADECIMIENTO
PROLOGO
ÍNDICE DE CONTENIDO
ÍNDICE DE TABLAS
ÍNDICE DE FIGURAS
GLOSARIO DE TÉRMINOS

CAPÍTULO I
INTRODUCCIÓN.....**1**
1.1 OBJETIVO.....3
1.2 OBJETIVOS ESPECÍFICOS.....3
1.3 ALCANCE DEL PROYECTO.....4

CAPÍTULO II
MARCO TEÓRICO.....**5**
2.1 ANTECEDENTES.....5
2.2 TIPOS DE REDES INALÁMBRICAS.....6
2.2.1 Redes inalámbricas de Corta Distancia.....6
2.2.2 Redes inalámbricas de Larga Distancia.....10
2.3 INTRODUCCIÓN A LAS REDES INALÁMBRICAS
DE ÁREA LOCAL (WLAN´s) 14
2.3.1 Evolución de WLAN.....15

2.3.2 Aplicaciones de las WLAN´s 16
2.3.3 Ventajas y desventajas de las WLAN´s 16
2.3.4 Cómo trabajan las WLAN´s 18
2.4 TOPOLOGÍAS DE LAS WLAN´s 20
2.4.1 WLAN´s Independientes (ad-hoc) 20
2.4.2 WLAN´s con Infraestructura 21
2.5 ESTÁNDARES DE LAS WLAN´s (IEEE 802.11) 22
2.5.1 802.11 legacy 23
2.5.2 802.11b 23
2.5.3 802.11a 23
2.5.4 802.11g 24
2.5.5 802.11e 24
2.5.6 802.11i 24
2.5.7 802.11d 25
2.5.8 802.11f 25
2.5.9 802.11h 25
2.6 SEGURIDAD EN LAS WLAN´s 26
2.6.1 Difusión de SSID 27
2.6.2 Filtrado de direcciones MAC 28
2.6.3 WEP (Wired Equivalent Privacy) 29
2.6.4 VPN (Virtual Private Network) 31
2.6.5 802.1x 33
2.6.6 WPA (Wi-Fi Protected Access) 34
2.7 COMPONENTES DE LAS WLAN´s 35
2.7.1 Modem/Routers ADSL-Cable 35
2.7.2 Wireless Routers 37
2.7.3 Access Points 38
2.7.4 Tarjetas de red Inalámbricas 40
2.7.5 Antenas 42
2.7.6 Amplificadores de señal 45
2.8 BANDAS DE FRECUENCIAS PARA WLAN 48

2.8.1 Banda ISM....48
2.8.2 Banda UNII....49
2.9 INTERFERENCIA Y ATENUACIÓN....50
2.9.1 Atenuaciones por solapamiento de la señal....51
2.10 MODELO DE CAPAS 802.11....52
2.10.1 Capa Física....53
2.10.2 Capa de Enlace de Datos....56

CAPÍTULO III

DISEÑO DE LA RED INALÁMBRICA....59

3.1 CRITERIOS DE DISEÑO DE LA RED. 59
3.2 SITUACIÓN ACTUAL DE LA RED....62
3.2.1 Dimensionamiento del edificio....62
3.2.2 Distribución....63
3.2.3 Materiales que componen el área de trabajo del edificio. 66
3.2.4 Esquemas de la red actual....67
3.2.5 Esquema de distribución física....68
3.2.6 Servicios de red que dispone la EMOP-Q: 69
3.3 DENSIDAD DE USUARIOS....70
3.3.1 Número de puntos de red y Host. 70
3.3.2 Requerimientos de los usuarios....70
3.4 PLANOS DEL EDIFICIO....71
3.5 SELECCIÓN DE EQUIPOS INALÁMBRICOS....78
3.5.1 Comparación entre marcas más destacadas....78
3.5.2 Selección de equipos....79
3.6 ACCESS POINT DWL-7200AP....80
3.6.1 Revision de Hardware....80
3.6.2 Características....82
3.7 MAPAS DE COBERTURA....83
3.7.1 Cobertura Horizontal....83
3.7.2 Cobertura vertical....89
3.8 DIRECCIONES IP PARA LA RED WLAN....96

3.8.1 Distribución de direcciones IP....98
3.8.2 Direcciones de ISP....99
3.9 CONFIGURACIÓN DE EQUIPOS....99
3.9.1 Inicio....100
3.9.2 Avanzado....103
3.9.3 Herramientas....114
3.9.4 Estado....118
3.9.5 Ayuda....120
3.10 SEGURIDAD....121
3.10.1 Servidor radius....121
3.11 RESUMEN DE CONFIGURACIONES....123
3.12 CONFIGURACIÓN DE ADAPTADORES INALÁMBRICOS....125
3.12.1 Características....125
3.12.2 Configuración del equipo....126
3.13 DISEÑO DE LA RED INALÁMBRICA....130

CAPÍTULO IV

SISTEMA DE SEGURIDAD CON CÁMARAS INALÁMBRICAS....132

4.1 CRITERIOS DE DISEÑO....132
4.2 SELECCIÓN DE CÁMARAS INALÁMBRICAS....133
4.3 CAMARA INALÁMBRICA DCS-2120....134
4.3.1 Requisitos de sistema....135
4.3.2 Características....136
4.3.3 Revisión de Hardware....136
4.4 DISEÑO DEL SISTEMA DE SEGURIDAD....139
4.5 CONFIGURACIÓN DEL EQUIPO....143
4.6 SOFTWARE PARA SISTEMA DE VIGILANCIA....149
4.6.1 Ventana de monitoreo....151
4.7 CONFIGURACIONES AVANZADAS....155
4.7.1 Audio/Video....156
4.7.2 Image Settings....157

4.7.3 Motion Detection.....158
4.8 RESUMEN DE CONFIGURACIONES.....159

CAPÍTULO V
ANÁLISIS DE COSTOS.....**161**
5.1 ANÁLISIS DE COSTOS PARA LA RED INALÁMBRICA.....161
5.1.1 Costos de equipos.....161
5.1.2 Costo de implementación y configuración.....162
5.2 ANÁLISIS DE COSTOS PARA EL SISTEMA DE SEGURIDAD.....163
5.2.1 Costos de equipos.....163
5.2.2 Costo de implementación y configuración.....163
5.3 COSTO TOTAL DEL PROYECTO.....164

CAPÍTULO VI
CONCLUSIONES Y RECOMENDACIONES.....**165**
6.1 CONCLUSIONES.....165
6.2 RECOMENDACIONES.....166

ANEXOS
ANEXO 1: DWL-7200AP Datasheet Access Point.
ANEXO 2: DWL- AG132 Datasheet Adaptador inalámbrico.
ANEXO 3: DCS – 2120 Datasheet Cámara IP inalámbrica.

REFERENCIAS BIBLIOGRÁFICAS
FECHA DE ENTREGA

ÍNDICE DE TABLAS

Tabla 2.1. Tecnologías inalámbricas.....14
Tabla 2.2. Descripción de estándares 802.11.....26
Tabla 2.3. Canales de la banda ISM.....49
Tabla 2.4. Materiales que provocan interferencia en las señales inalámbricas.....50
Tabla 3.1. Puntos de red y host´s habilitados en cada piso.....70
Tabla 3.2. Tabla comparativa de equipos inalámbricos.....79
Tabla 3.3. Configuraciones de access points.....123
Tabla 3.4. Configuraciones de direcciones IP para access points.....125
Tabla 4.1. Tabla comparativa de equipos.....134
Tabla 4.2. Alcance de lentes para cámaras.....139
Tabla 4.3. Resumen de configuraciones.....160
Tabla 5.1. Cotización de equipos para la red inalámbrica.....162
Tabla 5.2. Cotización de instalación para el sistema de red inalámbrica.....162
Tabla 5.3. Cotización de equipos para el sistema de seguridad.....163
Tabla 5.4. Cotización de instalación para el sistema de seguridad.....163
Tabla 5.5. Cotización de instalación del proyecto completo.....164

ÍNDICE DE FIGURAS

Figura 2.1. Red WPAN.....7
Figura 2.2. Red WLAN.....9
Figura 2.3. Red WMAN.....11
Figura 2.4. Red WWAN.....12
Figura 2.5. Estándares de redes WPAN, WLAN, WMAN y WWAN.....13
Figura 2.6. Onda Portadora de radiofrecuencia.....18
Figura 2.7. Onda modulada.....19
Figura 2.8. Configuración típica WLAN.....19
Figura 2.9. Red WLAN Independiente.....20
Figura 2.10. Red WLAN independiente extendida con access point como repetidor.....21
Figura 2.11. WLAN de Infraestructura.....22
Figura 2.12. Funcionamiento del algoritmo WEP en modalidad cifrado.....29
Figura 2.13. Funcionamiento del algoritmo WEP en modalidad descifrado.....30
Figura 2.14. Estructura de una VPN para acceso inalámbrico seguro.....32
Figura 2.15. Modem/Router Netgear.....36
Figura 2.16. Wíreles Router Linksys.....37
Figura 2.17. Access Point D-Link.....39
Figura 2.18. Tarjeta PCMCIA Belkin.....40
Figura 2.19. Adaptador PCMCIA.....40
Figura 2.20. Adaptador Wireless USB.....41
Figura 2.21. Tarjeta PCI 54 Mbps.....41
Figura 2.22. Antena unidireccional.....43
Figura 2.23. Antena Bidireccional.....43
Figura 2.24. Antena Bidireccional de doble banda 3Com.....44
Figura 2.25. Señal emitida de antena Omnidireccional.....44

Figura 2.26. Antena Omnidireccional de doble banda.....45
Figura 2.27. Amplificador 802.11b.....47
Figura 2.28. Amplificador 802.11g.....47
Figura 2.29. Efecto multitrayectoria.....51
Figura 2.30. Modelo OSI y IEEE 802.11.....52
Figura 2.31. Modelo OSI, IEEE 802.11 e IEEE 802.2.....53
Figura 2.32. Capa Física 802.11.....53
Figura 2.33. Sistema básico de comunicación digital Spread Spectrum.....54
Figura 2.34. Capa de Enlace de Datos 802.11.....56
Figura 2.35. Diagrama de flujo CSMA/CA.....58
Figura 3.1. Cobertura idealizada para access points en diferentes pisos.....60
Figura 3.2. Asignación de canales sin interferencia.....61
Figura 3.3. Modelo de Planta baja y primer piso.....62
Figura 3.4. Modelo del Segundo al sexto piso.....62
Figura 3.5. Esquema de la red actual.....67
Figura 3.6. Esquema de distribución física.....68
Figura 3.7. Planta Baja.....71
Figura 3.8. Primer Piso.....72
Figura 3.9. Segundo Piso.....73
Figura 3.10. Tercer Piso.....74
Figura 3.11. Cuarto Piso.....75
Figura 3.12. Quinto Piso.....76
Figura 3.13. Sexto Piso.....77
Figura 3.14. Panel frontal del access point D-Link DWL-7200AP.....80
Figura 3.15. Panel posterior access point D-Link DWL-7200AP.....81
Figura 3.16. Comando ping a 3 metros.....84
Figura 3.17. Nivel de señal y velocidad de conexión a 3 metros.....84
Figura 3.18. Comando ping a 6 metros.....85
Figura 3.19. Nivel de señal y velocidad de conexión a 6 metros.....85
Figura 3.20. Comando ping a 9 metros.....86
Figura 3.21. Nivel de señal y velocidad de conexión a 9 metros.....86

Figura 3.22. Comando ping a 12 metros.....87
Figura 3.23. Nivel de señal y velocidad de conexión a 12 metros.....87
Figura 3.24. Comando ping a ~15 metros.....88
Figura 3.25. Nivel de señal y velocidad de conexión a ~15 metros.....88
Figura 3.26. Esquema de Cobertura horizontal.....89
Figura 3.27. Comando ping a 3 metros.....90
Figura 3.28. Nivel de señal y velocidad de conexión a 3 metros.....90
Figura 3.29. Comando ping a 6 metros.....91
Figura 3.30. Nivel de señal y velocidad de conexión a 6 metros.....91
Figura 3.31. Comando ping a 9 metros.....92
Figura 3.32. Nivel de señal y velocidad de conexión a 9 metros.....92
Figura 3.33. Comando ping a 12 metros.....93
Figura 3.34. Nivel de señal y velocidad de conexión a ~15 metros….....93
Figura 3.35. Comando ping a ~15 metros.....94
Figura 3.36. Nivel de señal y velocidad de conexión a ~15 metros.....94
Figura 3.37. Esquema de Cobertura vertical.....95
Figura 3.38. Sensibilidad del equipo.....96
Figura 3.39. Esquema de Dirección de red y mascara de subred.....97
Figura 3.40. Browser Internet Explorer 6.0.....99
Figura 3.41. Inicio de sesión.....100
Figura 3.42. Menú Inicio – Asistente.....101
Figura 3.43. Menú Inicio – Inalámbrico.....101
Figura 3.44. Menú Inicio – LAN.....102
Figura 3.45. Menú Avanzado – Modo.....103
Figura 3.46. Menú Avanzado – Site Survey.....104
Figura 3.47. Menú Avanzado – Rendimiento.....105
Figura 3.48. Menú Avanzado – Filtros – Wireless access settings.....107
Figura 3.49. Menú Avanzado – Filtros – WLAN partition.....108
Figura 3.50. Menú Avanzado – Encriptación.....110
Figura 3.51. Menú Avanzado – DHCP server.....112
Figura 3.52. Menú Avanzado – DHCP server.....113

Figura 3.53. Menú Avanzado – DHCP server.....114
Figura 3.54. Menú Herramientas – Administración.....115
Figura 3.55. Menú Herramientas – Sistema.....115
Figura 3.56. Menú Herramientas – Firmware.....116
Figura 3.57. Menú Herramientas – Configuración de archivo.....117
Figura 3.58. Menú Herramientas – Misceláneo.....117
Figura 3.59. Menú Estado – Información del dispositivo.....118
Figura 3.60. Menú Estado – Estadísticas.....119
Figura 3.61 Menú Estado – Información del cliente.....120
Figura 3.62. Menú Ayuda.....120
Figura 3.63. Esquema de funcionamiento de Radius.....122
Figura 3.64. Adaptador DWL- AG132.....126
Figura 3.65. Utilitario del DWL- AG132.....127
Figura 3.66. Configuración DWL- AG132.....128
Figura 3.67. Configuración de direcciones IP y DNS.....128
Figura 3.68. Site Survey.....129
Figura 3.69. Site Survey - Configure.....129
Figura 3.70. Configuración de seguridad avanzada.....130
Figura 3.71. Diseño de red inalámbrica.....131
Figura 4.1. Panel frontal de la cámara D-Link DCS-2120.....137
Figura 4.2. Panel lateral de la cámara D-Link DCS-2120.....138
Figura 4.3. Panel posterior de la cámara D-Link DCS-2120.....138
Figura 4.4. Área de cobertura de la cámara.....140
Figura 4.5. Cobertura planta baja.....140
Figura 4.6. Cobertura primer piso.....141
Figura 4.7. Cobertura segundo piso.....141
Figura 4.8. Cobertura tercer piso.....141
Figura 4.9. Cobertura cuarto piso.....142
Figura 4.10. Cobertura quinto piso.....142
Figura 4.11. Cobertura sexto piso.....142
Figura 4.12. Instalación del software para configuración.....143

Figura 4.13. Network Camera installation....143
Figura 4.14. Información de firmware....144
Figura 4.15. Mensaje de actualización de firmware....145
Figura 4.16. Buscando cámaras....145
Figura 4.17. Configuración de cámaras....146
Figura 4.18. Configuración de red....147
Figura 4.19. Configuración de red (continuación)....148
Figura 4.20. Icono del explorador para la cámara IP....148
Figura 4.21. Instalación del sistema de vigilancia....150
Figura 4.22. Password del usuario admin....150
Figura 4.23. Pantalla principal de monitoreo....151
Figura 4.24. Pantalla principal de monitoreo....152
Figura 4.25. Misc. Functions....152
Figura 4.26. Channel area....153
Figura 4.27. Layout area....153
Figura 4.28. Área de 16 cámaras....154
Figura 4.29. Hard disck status....154
Figura 4.30. Hard disck status....154
Figura 4.31. DI/DO control....155
Figura 4.32. Alert message....155
Figura 4.33. Pantalla de Inicio de la cámara....156
Figura 4.34. Audio/Video....157
Figura 4.35. Image Settings....158
Figura 4.36. Motion detection....159

GLOSARIO DE TÉRMINOS

Ad-Hoc	WLAN independiente.
CMOS	Tipo de sensor de cámaras.
CSMA/CA	Acceso múltiple por detección de portadora con evasión de colisiones.
DHCP	Protocolo de configuración del host dinámico.
DSSS	Espectro Ensanchado de Secuencia Directa.
FHSS	Espectro Ensanchado con Saltos de Frecuencias.
ICV	Integrity Check Value (variable de chequeo de integridad).
ISM	Banda industrial, científica y médica.
LAN	Red de área local.
LUX	Unidad de medida de iluminación.
MAC	Control de acceso al medio.
OSI	Interconexión de sistemas abiertos.
OFDM	Modulación por división ortogonal de frecuencia.
POP	Protocolo de oficina de correos.
RADIUS	Remote Access Dial-In User Servise.
SSID	Service Set Identifier (“Seteo” de identificación de servicio).
UNII	Banda nacional no licenciada de información e infraestructura.
VPN	Red privada virtual.
WEP	Privacidad equivalente cableada.
Wi-Fi	Wireless Fidelity (fidelidad inalámbrica).
WLAN	Red inalámbrica de área local.
WMAN	Red inalámbrica de área metropolitana.
WPA	Acceso protegido Wi-Fi.
WPAN	Red inalámbrica de área personal.
WWAN	Redes inalámbricas de área amplia.

CAPÍTULO I

INTRODUCCIÓN

En la actualidad uno de los desarrollos tecnológicos que ha logrado captar la atención y el interés de muchas personas y empresas son las comunicaciones inalámbricas las cuales permiten comunicarse mediante conexiones de alta velocidad desde cualquier parte con los servicios que el usuario utilice en su entorno diario.

El término "inalámbrico" hace referencia a la tecnología sin cables que permite conectar varios equipos entre sí. El uso de la tecnología inalámbrica supone liberarse de los cables sin sacrificar las posibilidades de conexión. Las limitaciones de espacio y tiempo desaparecen, lo que significa que puede ubicarse una oficina en prácticamente cualquier lugar.

Las redes inalámbricas llevan años ofreciendo la posibilidad de unir puntos de difícil acceso y además permiten moverse libremente dentro de un entorno, en el cual el acceso a distintas áreas tenga una mayor dificultad al momento de usar cables, manteniendo la conectividad.

Estos servicios estaban restringidos a las grandes empresas pero actualmente, gracias a los últimos desarrollos que mejoran en velocidad, la consolidación y madurez de los estándares que definen estas redes y la ampliación de terminales más económicos desarrollados por varias empresas, hace que se abra cada vez más el marco de usuarios inalámbricos a grandes y medianas empresas, pequeños negocios e incluso a usuarios residenciales que ven en las tecnologías inalámbricas nuevas maneras de comunicarse de una manera más simple y segura.

Los dispositivos inalámbricos se conectan a otros dispositivos o puntos de acceso inalámbricos a fin de proporcionar a los trabajadores métodos más sencillos y transparentes. Las aplicaciones de oficina ayudan también a aligerar la carga de la red. El uso de la tecnología inalámbrica hace que la empresa aumente en eficacia y productividad. Los empleados pueden dedicarse a lo que saben hacer mejor, sin tener que batallar para superar obstáculos de tipo tecnológico.

Dado que las redes de datos ocupan un lugar muy importante en el desarrollo y competitividad de una empresa, es necesario conocer las tecnologías y la ingeniería que involucra brindar estos servicios en comunicaciones inalámbricas en lo referente a redes de datos y comunicación entre usuarios para la empresa.

Otro factor importante que se debe tomar en cuenta en redes inalámbricas es la seguridad. Al ser una tecnología sin cables existe una gran brecha abierta por la que personas ajenas puedan acceder a la información de la red. Para evitar esto, se utilizan diferentes métodos de seguridad, de acuerdo a la cantidad de tráfico y el tipo de información que se maneje en la empresa, que serán analizados detalladamente del desarrollo del proyecto.

La tecnología inalámbrica no se desarrolla únicamente el en ámbito de las redes LAN sino que también se desarrolla en distintos puntos de acción como por ejemplo los sistemas de seguridad que por medio de cámaras de video inalámbricas pueden dar seguridad visual a un hogar, edificio, campus, etc. este es otro punto que se tratará en este trabajo con el fin de satisfacer las necesidades de la empresa.

Los sistemas de seguridad inalámbricos son de gran ayuda para el usuario que necesita protección y control de sus pertenencias por lo que hoy en día se aplica mucho para seguridades de bienes personales y empresariales. Es así que la implementación de un sistema de seguridad mediante cámaras de video es una

buena opción para el monitoreo de edificios empresariales por los que a diario existe mucho flujo de personas.

1.1 OBJETIVO

El principal objetivo de este proyecto es diseñar la red de comunicaciones inalámbrica para el edificio de la Empresa Metropolitana de Obras Publicas de Quito (EMOP-Q) y un sistema de seguridad mediante cámaras de video inalámbricas con acceso remoto para la planta principal del edificio, así como también garantizar el correcto funcionamiento de los equipos inalámbricos que se utilizarán en estos diseños.

1.2 OBJETIVOS ESPECÍFICOS

- Analizar el funcionamiento y comportamiento de la tecnología inalámbrica aplicada a redes de área local (WLAN´s).
- Diseñar la red inalámbrica para la comunicación de datos entre usuarios de la red así como también con el proveedor de servicios de Internet de la Empresa.
- Investigar los distintos estándares inalámbricos que existen para desarrollar redes WLAN´s.
- Aplicar los protocolos de seguridad necesarios para la red a fin de que la información de la empresa no sea vulnerada.
- Conocer los tipos de equipos, y sus diferentes características, que pueden ser usados en el diseño de la red inalámbrica dependiendo de las necesidades de la red.
- Diseñar la estructura del sistema de seguridad inalámbrico basándose en planos arquitectónicos del edificio.
- Conocer los diferentes métodos y herramientas que existen para desarrollar sistemas de seguridad inalámbricos.
- Seleccionar los equipos más adecuados para el diseño del sistema de seguridad inalámbrica con monitoreo de cámaras remoto de acuerdo a la una comparación entre distintas marcas.

1.3 ALCANCE DEL PROYECTO

El proyecto consiste en diseñar una topología de red inalámbrica que cumpla con los requerimientos de la empresa de manera que todas las aplicaciones con las que la EMOP-Q trabaja en todas sus áreas tengan un correcto desempeño y funcionalidad, además de indicar las ventajas y desventajas que tienen las redes inalámbricas y el desarrollo que ha alcanzado esta tecnología desde su inicio hasta la actualidad.

Se pretende también dar a conocer las facilidades y los costes reducidos que presenta la instalación de ese tipo de redes y a la vez, conocer las características de funcionamiento y mantenimiento que se deben dar a cada uno de los equipos inalámbricos que se utilizarán en este diseño.

Al momento de hablar de tecnología inalámbrica debemos tener en cuenta que no es únicamente aplicable a redes de datos, es decir, transferencia de archivos, servicios de correo electrónico, Internet, etc., por lo que el diseño del sistema de seguridad inalámbrico es un ejemplo claro de una aplicación distinta pero usando la misma tecnología.

El diseño que se realizará tiene como objetivo primordial hacer una comparación de funcionalidad, y beneficios entre las redes de tipo cableadas y las de tipo inalámbricas, con lo cual podemos adquirir un criterio más definido al momento de decidir el tipo de tecnología que conviene implementar en determinadas circunstancias de trabajo.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES

La tecnología inalámbrica ocupa un espacio muy importante en la historia de las telecomunicaciones. Si nos remontamos en la historia, encontramos que la teoría de las comunicaciones inalámbricas empezó con la postulación de las ondas electromagnéticas por James Cleck Maxwell durante el año de 1860 en Inglaterra. Estas leyes fueron desarrolladas por algunos años y encontramos que en 1880 se logró la demostración de la existencia de estas ondas por Heinrich Rudolf Hertz.

A partir de estos estudios se han expuesto numerosos métodos y complementos teóricos para aplicar esta ciencia en el desarrollo de las comunicaciones inalámbricas que hasta el momento se las aplica en muchas actividades de la vida diaria como por ejemplo la radiodifusión que tuvo sus inicios en la década de 1920, la televisión y su control remoto desarrollada a partir del año 1930, procedimientos de rastreo de unidades vía satélite en una región en los años 1950, los teléfonos celulares en 1970 y hasta en juguetes como son los autos o aviones a control remoto.

En la actualidad una de las aplicaciones inalámbricas de mayor aceptación, y que se han desarrollado velozmente, es la que concierne a las “redes LAN inalámbricas (WLAN)”, ya que se obtienen altas velocidades de transmisión sin necesidad de tener un diseño de cableado estructurado en una determinada localidad y teniendo la posibilidad de compartir accesorios de oficina como fax, teléfonos, impresoras, scanners, etc.

Como se puede observar, la tecnología inalámbrica se ha venido desarrollando desde hace más de 80 años atrás brindando servicios básicos que son de gran necesidad y de uso diario para el usuario común facilitando su conectividad con el mundo, es por eso que en la actualidad ésta tecnología está invadiendo el mercado con mucha más fuerza y cada ves se vuelve más popular y accesible.

2.2 TIPOS DE REDES INALÁMBRICAS

Cada uno de los tipos de redes inalámbricas que se van a indicar funcionan bajo un estándar desarrollado por la IEEE, Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers), que es una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros en telecomunicaciones, ingenieros en electrónica, ingenieros en informática e ingenieros en computación.

La variedad en aplicación de las redes inalámbricas es muy amplia ya que van desde la interconexión de computadoras a cortas distancias hasta comunicaciones vía satélite que pueden llegar a cualquier parte del mundo, es por eso que las redes inalámbricas pueden clasificarse en dos categorías que son: *redes inalámbricas de corta distancia y redes inalámbricas de larga distancia.*

2.2.1 Redes inalámbricas de Corta Distancia

Este tipo de redes son utilizadas principalmente para comunicar equipos dentro de hogares, almacenes, hospitales, redes de campus u oficinas que no se encuentren muy retirados entre si. Dentro de esta clasificación encontramos dos tipos de redes inalámbricas que son:

- WPAN: Redes inalámbricas de área personal.
- WLAN: Redes inalámbricas de área local.

Redes WPAN (Wireless Personal Area Network)

Las Redes WPAN son redes que fueron desarrolladas para trabajar sobre áreas reducidas ya tienen menor cobertura y se usan para compartir una impresora, una cámara fotográfica o un scanner, PDA´s o un teléfono celular con una computadora y así poder intercambiar información. Estas redes se extienden a una distancia máxima de 10 metros y emplean tecnologías de comunicación inalámbrica de corto alcance. El gráfico siguiente muestra una red WPAN.

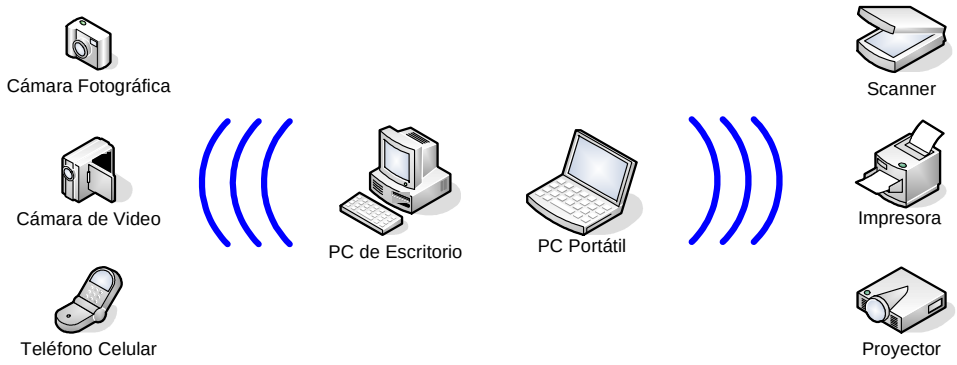


Figura 2.1. Red WPAN

Las redes WPAN usan la tecnología Bluetooth. El estándar bluetooth fue creado en 1994 por una asociación de grandes compañías entre las que se destacan: Intel, Motorola, Ericsson, Nokia, Microsoft e IBM. Transmite la información empleando ondas de radio sobre la frecuencia pública 2,4 GHz.

La IEEE ha desarrollado el protocolo 802.15 para las redes WPAN con el objetivo de lograr la interoperabilidad con otros dispositivos inalámbricos. Las características generales del estándar 802.15 son:

- Tecnología inalámbrica para distancias no excedentes a 10 metros, alcanzando velocidades del rango de 1Mbps.
- Comunicación automática. La estructura de los protocolos que lo forman favorece la comunicación automática sin necesidad de que el usuario la inicie.

- Bajo consumo de potencia. Lo pequeño de los dispositivos y su portabilidad requieren de un uso adecuado de la energía, el cual provee esta tecnología.
- Su operación se efectúa bajo una banda de frecuencias no licenciada (2.4GHZ), lo que ayuda a su bajo costo.
- Integración de servicios. Puede soportar transmisiones de voz y datos de manera simultánea.
- Transmisión omnidireccional. Debido a que basa su comunicación en radiofrecuencia, no requiere línea de vista y permite configuraciones punto-multipunto.
- Utiliza modulación Spread Spectrum Frequency Hopping como técnica de multiplexaje, lo que disminuye el riesgo de que las comunicaciones sean interceptadas o presenten interferencia con otras aplicaciones.
- Provee especificaciones para autenticar dispositivos que intenten conectarse a la red Bluetooth, así como cifrado en el manejo de llaves para proteger la información.
- Tiene la característica de formar redes en una topología donde un dispositivo hace las veces de maestro y hasta siete más operando como esclavos.

Redes WLAN (Wireless Local Area Network)

Las redes WLAN disponen de un alcance más amplio, tienen mayor cobertura ya que con su tecnología más desarrollada logra cubrir áreas de 300 metros con línea de vista y hasta 100 metros en sitios que tienen obstáculos. Se aplican para realizar transmisión y recepción de información dentro de una red de área local (LAN).

Este tipo de redes son empleadas para conectar usuarios móviles o usuarios estáticos de difícil acceso físico a redes corporativas de forma inalámbrica. Emplean equipos denominados “estaciones base” o “puntos de acceso” (access points) como puentes de conexión entre la red inalámbrica y la red cableada. Requieren NIC´s (Tarjeta de interfaz de red) especiales en los clientes (PC´s,

PDA´s o notebooks) para efectuar la comunicación. El gráfico siguiente muestra una red WLAN.

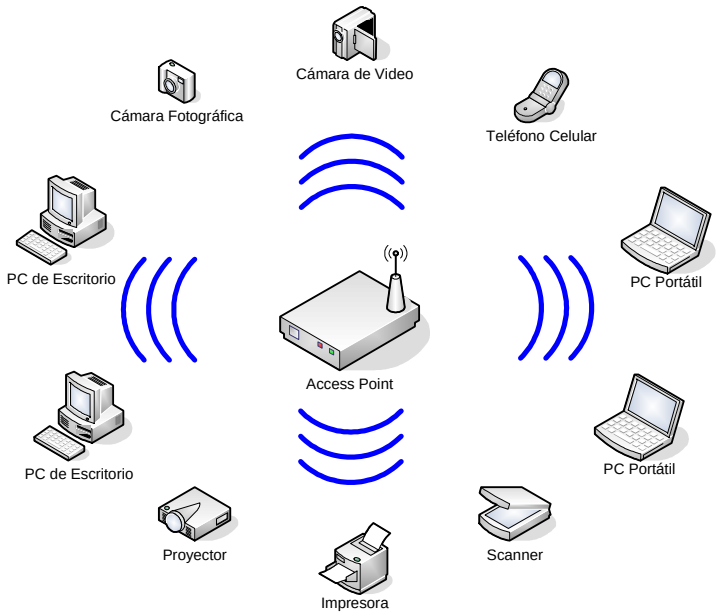


Figura 2.2. Red WLAN

La tecnología base que usan las redes WLAN es la denominada “Wi-Fi” que es una abreviatura de “Wireless Fidelity”. La tecnología WLAN viene regida por el estándar 802.11, especificado por el IEEE. Mediante este proceso, se garantiza inicialmente la interoperabilidad entre diferentes fabricantes y un funcionamiento dentro de las capas del modelo de comunicaciones igual que cualquier otra tecnología de LAN. En la actualidad podemos encontrarnos de manera general con dos tipos de comunicación Wi-Fi:

- 802.11b, velocidad de transmisión de 11 Mbps.
- 802.11g, velocidad de transmisión de 54 Mbps.

Wi-Fi opera en las banda pública de 2.4 y 5 GHz y tiene un alcance promedio de 100 a 300 metros, trabaja bajo modulación OFDM y Spread Spectrum en sus estándares 802.11b y g lo que le convierte en una tecnología muy confiable para la transmisión de datos.

2.2.2 Redes inalámbricas de Larga Distancia

Estas redes se utilizan para transmitir información en espacios mucho más grandes que pueden variar desde una misma ciudad o hasta varios países y son normalmente utilizadas para realizar videoconferencias, transmisiones de canales de televisión, etc. En esta categoría tenemos dos tipos de redes que son:

- WMAN: Redes inalámbricas de área metropolitana.
- WWAN: Redes inalámbricas de área amplia.

Redes WMAN (Wireless Metropolitan Area Network)

Las redes WMAN son más extensas ya que pueden cubrir una distancia mucho mayor que las WLAN, aproximadamente unos 50 kilómetros, conectando edificios entre sí dentro de una amplia área geográfica. Este tipo de redes son ideales para enlazar 2 o mas redes LAN permitiendo así a las empresas transferir información a grandes distancias.

Podría considerarse entonces a las MAN como un subconjunto de las WAN con mayor aplicación en la constitución de redes privadas o redes corporativas.

La tecnología Wi-Max, que es la abreviatura de Worldwide Interoperability for Microwave Access, es la que utilizan las redes WMAN, esta tecnología utiliza el estándar de la IEEE 802.16. Este estándar de comunicaciones permite transmitir información a velocidades de hasta 124 Mbps y tiene un alcance de 50 kilómetros. WiMAX es una tecnología inalámbrica basada en estándares que ofrece conectividad de banda ancha de alta velocidad de última milla para hogares y empresas y para redes inalámbricas móviles. El gráfico siguiente muestra una red WMAN.

(SIGUIENTE HOJA)

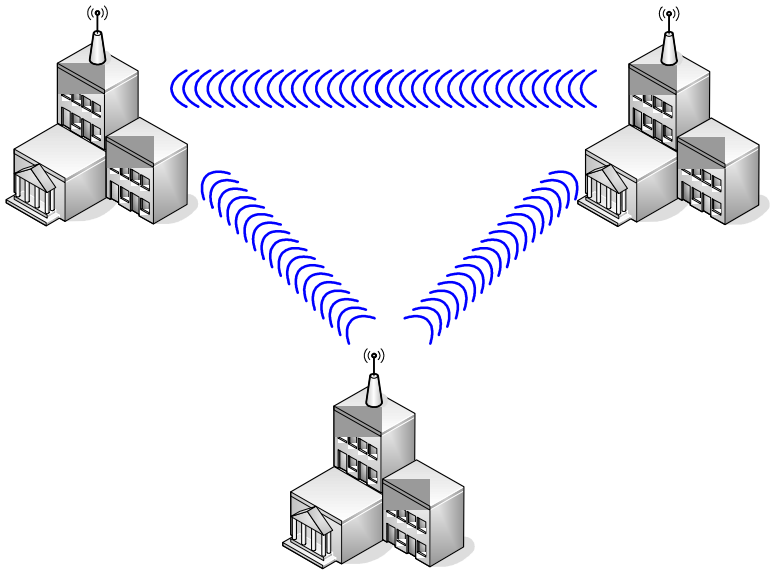


Figura 2.3. Red WMAN

El estándar IEEE 802.16 hace referencia a un sistema BWA (Broadband Wireless Access) de alta tasa de transmisión de datos y largo alcance escalable, y que permite trabajar en bandas del espectro tanto "licenciado" como "no licenciado". El servicio, tanto móvil como fijo, se proporciona empleando antenas sectoriales tradicionales o bien antenas adaptativas con modulaciones flexibles que permiten intercambiar ancho de banda por alcance.

Este sistema funciona de manera similar a las actuales redes inalámbricas de tecnología Wi-Fi, en donde una estación base con una antena (access point) controla el acceso inalámbrico de los equipos a la red. Las principales características del estándar WiMax 802.16 son:

- Utilización de técnicas de multiplexación OFDM y un sistema MIMO de antenas para alcanzar una velocidad de transmisión de hasta 124 Mbps, es decir más del doble que la máxima ofrecida por Wi.Fi.
- OFDM es un método que permite transmitir una señal a gran velocidad a través de un medio hostil, brindando protección, en la medida de lo posible,

contra interferencias tales como el eco causado por reflexiones de la señal transmitida.

- Amplio radio de acción de 50 Km. hasta 70 Km., considerablemente mayor que los 300 metros máximos permitidos por Wi-Fi, por lo que se reduce el número de antenas necesarias para establecer una red WiMAX, convirtiendo a esta tecnología en una función especialmente atractiva para redes rurales.
- Adicionalmente, WiMAX es que soporta las llamadas antenas inteligentes, lo cual mejora la eficiencia espectral.

Redes WWAN (Wireless Wide Area Network)

Las tecnologías WWAN permiten a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como ciudades o países, mediante el uso de antenas en varias ubicaciones o sistemas satélite que mantienen los proveedores de servicios inalámbricos. Las tecnologías WWAN actuales se conocen como sistemas de segunda generación (2G). Entre los sistemas 2G principales se incluyen Global System for Mobile Communications (GSM), Cellular Digital Packet Data (CDPD) y Code Division Multiple Access (CDMA). El gráfico muestra una red WWAN típica.

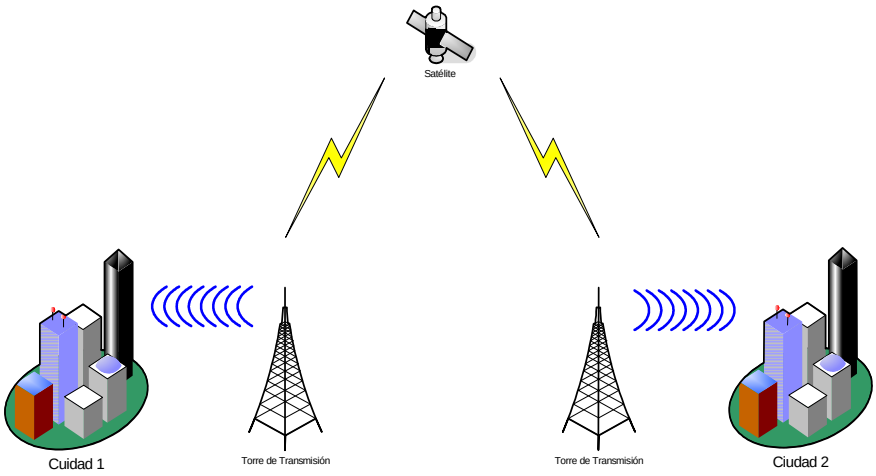


Figura 2.4. Red WWAN

Las tecnologías con las que disponen las redes WWAN basadas en sistemas celulares son las siguientes:

- CDPD (Celular Digital Packet Data): trabaja basado en la conmutación de paquetes sobre redes TDMA (Time Division Multiple Access) y ofrece velocidades máximas de 19.2 Kbps.
- CDMA (Code Division Multiple Access): En su versión CDMAOne soporta transferencia de datos con velocidades hasta de 64Kbps, en su última versión CDMA2000 maneja velocidades entre 307 Kbps y 2.4 Mbps.
- GPRS (General Packet Radio Service): opera sobre redes GSM a velocidades teóricas de 171.2 Kbps.
- EDGE (Enhanced Data Rates for Global Evolution): especificación que busca superar las tasas de transferencia de datos hasta 384 Kbps
- 3GSM: La más reciente versión de GSM. Ofrece velocidades de 144 Kbps en condiciones de alta movilidad (mayores a 120 Km/h), 384 Kbps en movilidad media (menores a 120 Km/h) y hasta 2 Mbps en condiciones de movilidad limitada (menores a 10 Km/h).

Una vez analizado cada tipo de red de una forma general, se presentan a continuación un gráfico que se muestra la cobertura que tiene cada tipo de red y su estándar característico:

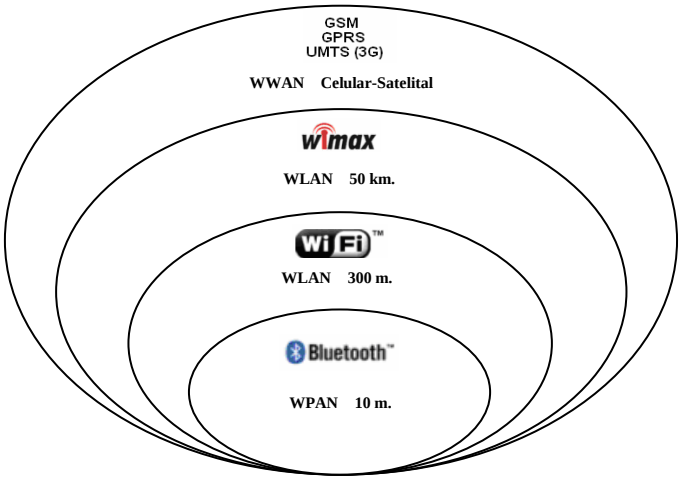


Figura 2.5. Estándares de redes WPAN, WLAN, WMAN y WWAN

La tabla que se muestra a continuación es una tabla comparativa que indica a manera de resumen las características de cada una de las tecnologías que comprenden las redes inalámbricas que fueron expuestas anteriormente, indicando su estándar, ancho de banda, alcance y aplicaciones:

	WPAN	***WLAN***	***WMAN***	***WWAN***
Estándares	802.15	802.11	802.16	802.20
Tecnologías	Bluetooth	Wi-Fi	Wi-Max	CDMA, GSM, GPRS
Ancho de Banda	Menor a 1 Mbps.	De 1 a 54 Mbps.	124 Mbps.	9.6 Kbps. a 2.4 Mbps.
Aplicaciones	Doméstica, PDA´s, Entorno de oficina	Redes Corporativas	Interconexión de Redes Corporativas	Telefonía móvil, celular, Satélite.

Tabla 2.1. Tecnologías inalámbricas

Luego de haber analizado las funciones y características básicas de cada tipo de red inalámbrica nos damos cuenta que el desarrollo del presente proyecto recae sobre el grupo de las redes WLAN y la tecnología Wi-Fi ya que se realizará el estudio para un edificio empresarial que consta con alrededor de 200 usuarios y requiere de distintos servicios que serán detallados en el capítulo siguiente. Por ésta razón es que a continuación se presenta de una manera más detallada la evolución, teoría y el funcionamiento de las redes WLAN

2.3 INTRODUCCIÓN A LAS REDES INALÁMBRICAS DE ÁREA LOCAL (WLAN´s)

En esta parte del proyecto se analizarán las propiedades, características, ventajas y desventajas de toda la tecnología que involucra el funcionamiento de una red inalámbrica de área local empezando desde el descubrimiento de este tipo de redes así como también las ventajas y desventajas que tienen los servicios inalámbricos.

2.3.1 Evolución de WLAN

Una wireless LAN es un sistema de comunicaciones que transmite y recibe datos utilizando ondas electromagnéticas y antenas en lugar del cable de par trenzado, coaxial o fibra óptica utilizado en las redes de área local convencionales, y que proporciona conectividad inalámbrica dentro de un edificio, de una pequeña área residencial o urbana, etc.

El origen de las WLAN se remonta al año 1979 al momento que se publican los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados por el IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema de espectro expandido (spread spectrum). En mayo de 1985, y tras cuatro años de estudios, la FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4735 GHz, 5,725-5,850 GHz para uso en las redes inalámbricas basadas en Spread Spectrum (SS), con las opciones DS (Direct Sequence) y FH (Frequency Hopping). Spread Spectrum es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea muy pocas interferencias.

Desde 1985 hasta 1990 se siguió trabajando en el desarrollo de las WLAN´s, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbit/s, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

2.3.2 Aplicaciones de las WLAN´s

En la actualidad las redes WLAN han encontrado una gran variedad de nuevos escenarios de aplicación tanto en el ámbito residencial como en entornos públicos, más allá de su origen corporativo. Estas aplicaciones son:

- **Escenario Residencial*:*** Una línea telefónica convencional terminada en un MODEM ADSL, que da servicio de Internet dedicado, se conecta a un access point para formar una red WLAN que ofrece cobertura a varios ordenadores en el hogar.
- **Redes Corporativas:** Una serie de Puntos de Acceso distribuidos en varias áreas de la empresa conforman una red WLAN autónoma o complementan a una LAN cableada. Son aplicaciones de alta densidad de tráfico con altas exigencias de seguridad.
- **Acceso a Internet en establecimientos públicos:** En estos establecimientos se ofrece a los clientes una tarjeta inalámbrica (NIC) que permiten acceso a Internet desde sus propias portátiles o PDA's. Es un escenario de acceso, involucrando un bajo número de Puntos de Acceso, parecido al residencial, pero que necesita mayores funcionalidades en el núcleo de red.
- **WLAN para cobertura de "Hot Spots":** Estas redes cubren áreas donde se concentra un gran número de usuarios de alto tráfico como son aeropuertos, estaciones de ferrocarril, centros de reuniones, etc. La red a instalar requiere un elevado número de Puntos de Acceso así como importantes exigencias de seguridad, gestión de red, facilidades de facturación, etc.

2.3.3 Ventajas y desventajas de las WLAN´s

Las redes WLAN ofrecen las siguientes ventajas en productividad, servicio, conveniencia y costos sobre las redes cableadas tradicionales:

Movilidad, productividad y servicios: Los sistemas WLAN proveen a los usuarios LAN acceso en tiempo real a cualquier tipo de información que se encuentre en una organización. Esta movilidad respalda la productividad y los

servicios que no son posibles con las redes cableadas. La posibilidad de conexión sin hilos entre diferentes dispositivos elimina la necesidad de compartir un espacio físico común y soluciona las necesidades de los usuarios que requieren tener disponible la información en todos los lugares por donde puedan estar trabajando.

Rápida instalación y simplicidad: La instalación de sistemas WLAN es rápida y fácil y puede eliminar la necesidad de pasar cable por las paredes y techos mejorando así el aspecto y la movilidad de locales y oficinas. También permite acceso instantáneo a usuarios temporales de la red.

Flexibilidad de instalación: La tecnología inalámbrica permite que la red se vaya donde el cable no puede llegar, superando mayor número de obstáculos. Así, es útil en zonas donde el cableado no es posible o es muy costoso.

Coste de propiedad reducido: Mientras que la inversión inicial requerida para el hardware de las WLAN´s puede ser más alta que la del hardware para una LAN cableada, los costos de instalación y gastos de ciclo de vida pueden ser significativamente más bajo. Los beneficios de coste a largo plazo son más grandes en ambientes que requieren movimientos dinámicos frecuentes, adición de equipos y usuarios y cambios.

Escalabilidad: Los sistemas WLAN's pueden ser configurados en una variedad de topologías para cubrir las necesidades de aplicaciones específicas e instalaciones. Las configuraciones son fácilmente cambiadas y se extienden de redes independientes apropiadas para una pequeña cantidad de usuarios a redes de infraestructuras completas de miles de usuarios que permiten comunicación sobre un área amplia.

Por otro lado la principal desventaja que enfrentan las redes inalámbricas es su velocidad de transmisión, anteriormente indicamos que la velocidad máxima de transmisión es de 54 Mbps., velocidad que puede no ser suficiente para las diversas aplicaciones empresariales en relación con la velocidad en una red

cableada puede alcanzar hasta 100 Mbps., razón por la cual el análisis de tráfico y servicios de red es muy importante.

2.3.4 Cómo trabajan las WLAN´s

Las LAN´s inalámbricas usan ondas electromagnéticas aéreas (ondas de radio) para transportar información desde un punto a otro sin depender de ninguna otra conexión física.

Las ondas de radio son a menudo enviadas como ondas portadoras de radio, es decir, son una forma de onda que serán moduladas por una señal en la que encuentran los datos que se van a transmitir. Las ondas portadoras son el medio a través del cual se transporta información a un receptor remoto. El gráfico representa una onda portadora:

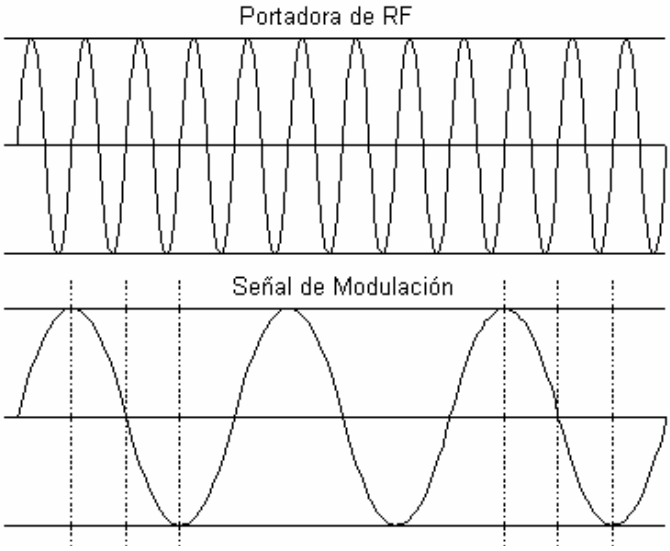


Figura 2.6. Onda Portadora de radiofrecuencia

Los datos a ser transmitidos son superpuestos en las portadoras de radio y pueden ser extraídas con exactitud por el receptor final. Este proceso se denomina modulación de portadora. En cuanto los datos son superpuestos en la portadora de radio, la señal de radio utiliza más de una frecuencia simple desde que la frecuencia es añadida a la portadora. La onda modulada se representa así:

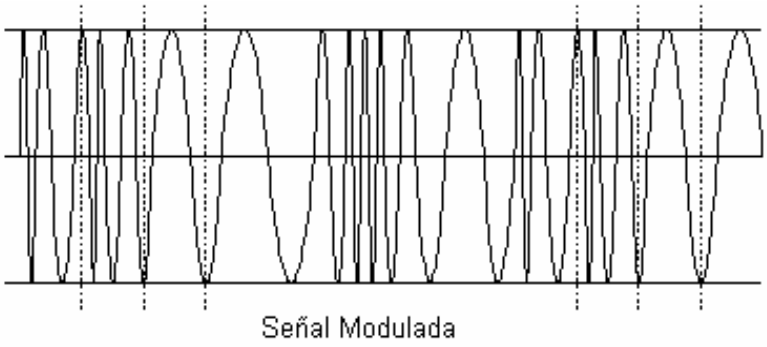


Figura 2.7. Onda modulada

Para extraer los datos enviados en los paquetes de información, el receptor de radio sintoniza (o selecciona) una frecuencia de radio mientras rechaza todas las otras señales con diferentes frecuencias. En la configuración típica de las WLAN, el dispositivo Transmisor/Receptor llamado *access point*, se conecta a la red cableada desde una ubicación fija que usa el cable estándar Ethernet (RJ 45). El access point recibe y transmite datos entre la WLAN y la red cableada. La siguiente figura muestra una configuración WLAN típica utilizando la infraestructura de una red cableada.

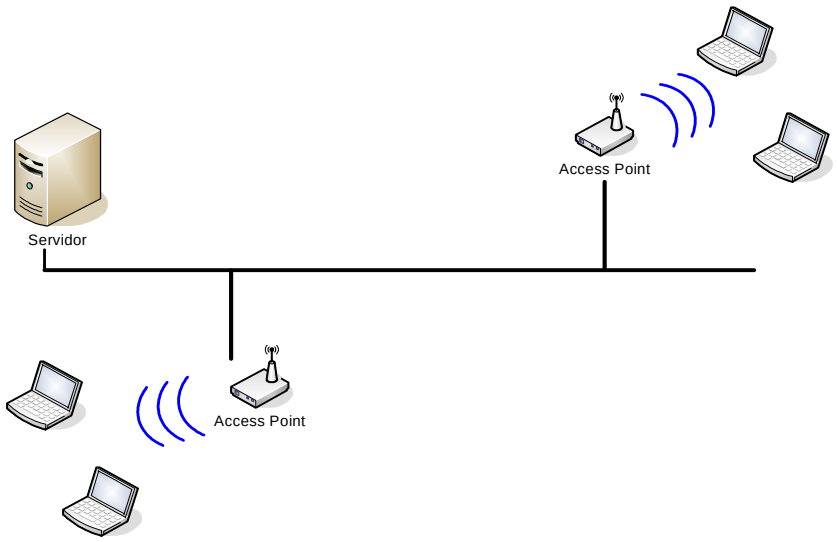


Figura 2.8. Configuración típica WLAN

2.4 TOPOLOGÍAS DE LAS WLAN´s

Las redes inalámbricas de área local tienen dos tipos de topologías definidas que son: Redes independientes (Ad-hoc) y redes de infraestructura.

2.4.1 WLAN´s Independientes (ad-hoc)

La configuración más simple es una WLAN independiente o “punto a punto” (peer to peer) que conecta un grupo de PC´s con adaptadores inalámbricos. En cualquier momento dos o más adaptadores inalámbricos están dentro del rango de cobertura entre ellos, esto se considera como una red independiente.

Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de la red punto a punto para lo cual únicamente se requiere disponer de un SSID (Service Set Identifier), que es “el nombre de la red”, igual para todos los nodos. Este tipo de redes no necesitan administración o pre-configuración, lo que las hace independientes. El gráfico ilustra una red de este tipo.

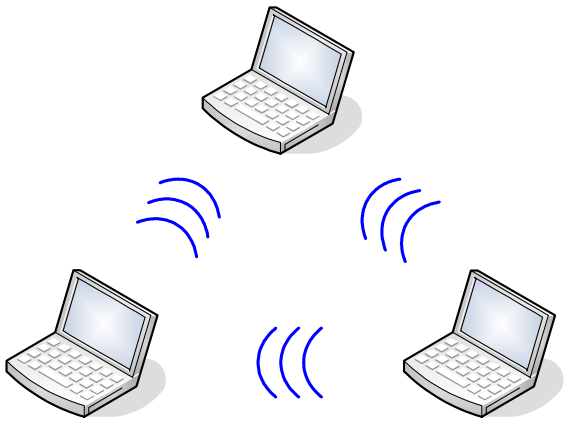


Figura 2.9. Red WLAN Independiente

Un access point puede extender el rango de funcionamiento de la WLAN´s independientes cuando es activado como un repetidor como indica la figura. El access point puede doblar la distancia de cobertura entre las PC´s inalámbricas como muestra la siguiente figura.

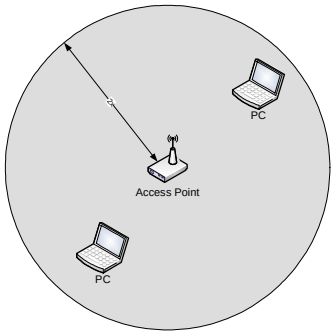


Figura 2.10. Red WLAN independiente extendida con access point como repetidor

El SSID es un código incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos

Existen algunas variantes principales del SSID. Las redes ad-hoc utilizan el BSSID (Basic Service Set Identifier); mientras que en las redes infraestructura, que se describen a continuación, se utiliza el ESSID (Extended Service Set Identifier).

2.4.2 WLAN´s con Infraestructura

En las WLAN´s con infraestructura, varios access points enlazan la WLAN con la red cableada y permite que usuarios compartan eficientemente recursos de la red.

Los access points no proveen únicamente comunicación con la red cableada sino que también mide el tráfico de red inalámbrico en la celda inmediata. Varios access points pueden suministrar cobertura inalámbrica para un edificio entero o un campus como demuestra la figura.

(SIGUIENTE HOJA)

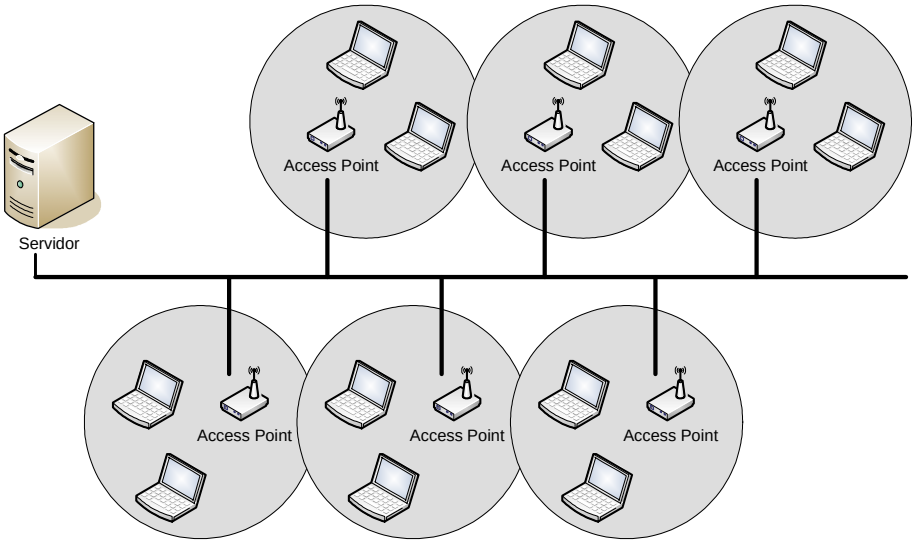


Figura 2.11. WLAN de Infraestructura

2.5 ESTÁNDARES DE LAS WLAN´s (IEEE 802.11)

El IEEE ha definido un conjunto de estándares para el entorno de la gestión de las redes inalámbricas bajo la denominación 802.11 que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Actualmente la familia del 802.11 se divide en 9 protocolos que son descritos a continuación:

Estándares inalámbricos.

- 802.11 legacy
- 802.11b
- 802.11a
- 802.11g

Extensiones de Estándares Inalámbricos.

- 802.11e
- 802.11i
- 802.11d
- 802.11f
- 802.11h

2.5.1 802.11 legacy

Ancho de banda máximo de hasta 2 Mbps. Opera en el espectro de 2.4 GHz sin necesidad de licencia. Posible interferencia con hornos microondas, dispositivos bluetooth, y teléfonos que usan la banda de 2.4GHz, puesto que operan en el mismo espectro de frecuencias. Utiliza sistemas de modulación FHSS (Espectro Ensanchado con Saltos de Frecuencias) y DSSS (Espectro Ensanchado de Secuencia Directa).

Una de las mayores debilidades de este estándar fue que dejaba mucha libertad de implementación a los proveedores de equipos, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas.

2.5.2 802.11b

Ancho de banda máximo de hasta 11Mbps. Opera en el espectro de 2.4 GHz. sin necesidad de licencia. Las mismas interferencias que para 802.11 legacy. Conocido como WIFI. Utiliza modulación DSSS Compatible con los equipos DSSS del estándar 802.11.

2.5.3 802.11a

Ancho de banda máximo de hasta 54 Mbps. Opera en el espectro de 5 GHz. sin necesidad de licencia. Es un estándar menos saturado. No es compatible con 802.11b y 802.11g. Utiliza modulación OFDM.

Dado que la banda de 2,4 Ghz tiene gran uso, el utilizar la banda de 5 GHz. representa una ventaja del estándar 802.11a, ya que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas por que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

2.5.4 802.11g

Ancho de banda máximo de hasta 54 Mbps. Opera en el espectro de 2.4 GHz. sin necesidad de licencia. Utiliza modulación DSSS y OFDM.

Es compatible con el estándar 802.11b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar 802.11g la presencia de nodos bajo el estándar 802.11b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar 802.11b.

2.5.5 802.11e

Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN. Se aplicará a los estándares físicos a, b y g de 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e.

2.5.6 802.11i

Se refiere al objetivo más frecuente del estándar 802.11, la seguridad. Se aplicará a los estándares físicos a, b y g de 802.11 Proporciona una alternativa a la Privacidad Equivalente Cableada (WEP) con nuevos métodos de encriptación y procedimientos de autentificación.

2.5.7 802.11d

Constituye un complemento al nivel de control de Acceso al Medio (MAC) en 802.11 para proporcionar el uso, a escala mundial, de las redes WLAN. Permitirá a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

2.5.8 802.11f

Su objetivo es lograr la interoperabilidad de Puntos de Acceso dentro de una red WLAN mutiproveedor. El estándar define el registro de Access Points dentro de una red y el intercambio de información entre dichos Access Points cuando un usuario se traslada desde un punto de acceso a otro.

2.5.9 802.11h

El objetivo es cumplir los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tengan control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

En la siguiente tabla se presenta un resumen de cada uno de los estándares del 802.11:

ESTÁNDAR	***DESCRIPCIÓN***
802.11 Legacy	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11 b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11 a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.

802.11 g	Establece una técnica de modulación adicional para la banda 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11 e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11 i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación.
802.11 d	Define un complemento al nivel de control de acceso al medio.
802.11 f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11 h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.

Tabla 2.2. Descripción de estándares 802.11

2.6 SEGURIDAD EN LAS WLAN´s

Cuando hablamos de redes inalámbricas debemos tener muy en cuenta que en cualquier configuración de este tipo de redes hay la posibilidad de que existan intrusos que quieran vulnerar o violentar la información de los usuarios que se encuentran en dicha red.

Las redes inalámbricas necesitan protección que en las redes cableadas son obviadas. Un intruso que busque acceso a una LAN cableada se enfrenta irremediablemente con el problema del acceso físico a la misma ya que para ingresar a la red necesita conectar su cable al switch o un punto de red a diferencia de una WLAN que únicamente basta permanecer en el área de cobertura para estar en contacto con la red. Esta situación obliga a la búsqueda de nuevas soluciones para garantizar la seguridad de los usuarios.

También debemos tener en cuenta lo que se quiere decir con seguridad, La seguridad viene dada por tres conceptos básicos e importantes que son:

- Autenticidad: El usuario no es un usuario desconocido.
- Privacidad: La información no es legible por terceros.
- Integridad: La información no puede ser alterada en tránsito.

Para garantizar que una red inalámbrica sea segura se debe cumplir con los siguientes requisitos:

- Las ondas de radio deben limitar o encapsular tanto como sea posible. Esto es difícil de lograr totalmente ya que las ondas de radio se dispersan por el aire, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la vez constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva, es decir, la red debe ser protegida para que los equipos no la reconozcan como una red abierta y puedan conectarse a ella.

Existen varios métodos para proteger una red inalámbrica, cada uno de estos presenta un nivel distinto de protección para la red así mismo como sus ventajas y desventajas características. Estas son algunas formas de maximizar la seguridad de una red inalámbrica y proteger los datos de intrusiones indeseadas:

- Difusión de SSID.
- Filtrado de direcciones MAC.
- WEP (Wired Equivalent Privacy).
- WPA (Wi-Fi Protected Access).
- VPN (Virtual Private Network).
- 802.1x

2.6.1 Difusión de SSID

Como se explico anteriormente, el SSID (Service Set IDentifier) es el “nombre” con el que se le conoce a una red inalámbrica, la difusión de SSID pretende únicamente no difundir u “ocultar” el SSID de la red, de esta forma, el

nombre de la red estará oculto ante los ojos de computadoras que hacen un barrido con sus adaptadores Wi-Fi para detectar la presencia de redes inalámbricas. Este tipo de seguridad tiene un nivel muy bajo de protección, y únicamente es una propiedad que tienen los equipos inalámbricos, generalmente los Access Points.

2.6.2 Filtrado de direcciones MAC

Este método consiste el crear una tabla de datos en cada uno de los access point de la red. En esta tabla constan las direcciones MAC (Media Access Control) de todas las tarjetas de red que pueden acceder al access point. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo para que pueda conectarse a la red.

Este método es muy sencillo y se puede aplicar en redes caceras o en pequeñas redes que no tengan un elevado tráfico de datos. Pero al ser un método de seguridad muy sencillo se hace impractico para el uso en redes medianas o grandes (infraestructura) ya que posee muchas desventajas que a continuación se indican.

- No produce una escalabilidad apropiada ya que cada una de las direcciones MAC de los equipos que se quieran autorizar para ingresar a la red debe ser previamente registrada en las tablas de datos de cada uno de los puntos de acceso de la red y cada vez que se desee dar de baja a un equipo, es necesario editar todas las tablas de direcciones. Mientras aumenta el número de access point o de usuarios de la red la situación se torna inmanejable.
- El formato de una dirección MAC no es amigable (normalmente se escriben 6 bytes en hexadecimal), y al momento de que existan muchos equipos en la red se puede llegar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas registradas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack o

WellenReiter, entre otros. De este modo, el atacante puede hacerse pasar por un usuario válido de la red.

Se debe notar además, que estos dos métodos no garantizan la confidencialidad de la información transmitida ya que no proveen ningún mecanismo de cifrado para la protección de la información. Los siguientes métodos si proveen un mecanismo de cifrado por lo que, a más de ser un método de protección, son protocolos de seguridad de 802.11.

2.6.3 WEP (Wired Equivalent Privacy)

WEP, privacidad equivalente a la cableada, es un algoritmo que forma parte del estándar 802.11 y fue diseñado para proteger los datos que se transmiten en forma inalámbrica mediante cifrado, WEP opera a nivel 2 del modelo OSI (capa de red) y sus objetivos, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

El cifrado del protocolo WEP se describe en el gráfico.

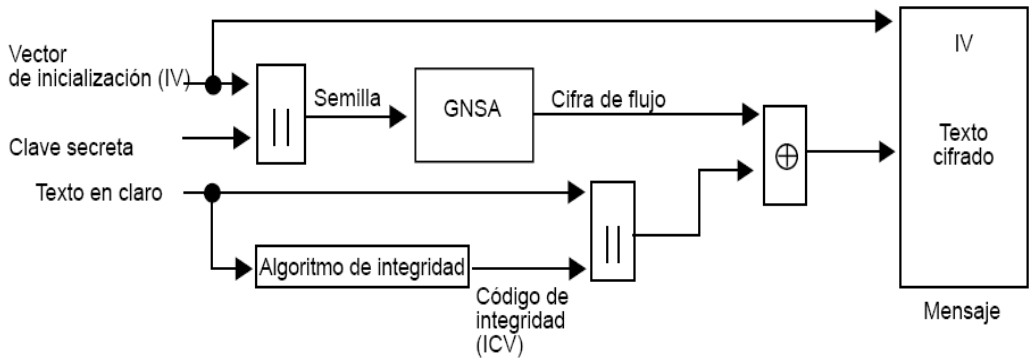


Figura 2.12. Funcionamiento del algoritmo WEP en modalidad cifrado

Al texto en claro (trama de información) se le procesa con un código de integridad ICV (Integrity Check Value) mediante el algoritmo CRC-32. Este ICV se concatena con la trama y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

Se escoge una clave compartida entre emisor y receptor para realizar el cifrado. Si esta clave se empleara siempre para cifrar las tramas, en algún momento llegaríamos a tener dos tramas iguales y por lo tanto dos tramas cifradas iguales, para evitar esto, se concatena la clave secreta con un numero aleatorio llamado Vector de Inicialización (IV) de 24 bits el cual va cambiando con cada trama que va a ser transmitida.

La Clave secreta y el IV (semilla) se concatenan y entran a un generador de números seudo-aleatorios llamado RC4 el cual es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

Una vez obtenidas la secuencia de clave y la trama se hace un XOR (o exclusivo) entre ellas y se obtiene como resultado la trama cifrada. El IV y la trama cifrada se transmiten juntos para efectos de decodificación de la trama.

Para realizar la decodificación se utiliza el siguiente esquema:

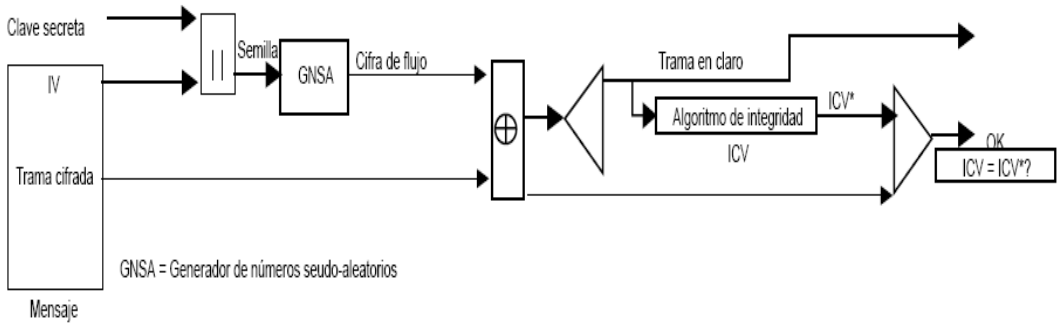


Figura 2.13. Funcionamiento del algoritmo WEP en modalidad descifrado.

En el receptor se utiliza el IV recibido y la clave secreta compartida (que es la misma en el emisor y receptor) para generar la misma “semilla” que se utilizó en el transmisor y por medio de otro generador RC4 se genera la cifra de flujo a partir

de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.

Se realiza una función XOR bit por bit de la cifra de flujo y la trama cifrada obteniéndose de esta manera la trama en claro y el ICV. A la trama en claro se la aplica el algoritmo CRC-32 para obtener un segundo ICV el cual se compara con el ICV recibido, si los dos IVC son iguales la trama es aceptada de lo contrario la trama se rechaza.

El protocolo WEP consta de dos tipos de encriptación: WEP de 64 bits y WEP de 128 bits.

WEP de 64 bits:

WEP de 64 bits se introdujo con la encriptación de 64 bits, que incluye un largo de clave de 40 bits, más 24 bits adicionales de datos generados por el sistema (64 bits en total). Algunos fabricantes de hardware se refieren a la encriptación de 64 bits por el nombre de encriptación de 40 bits. Poco después de lanzarse al mercado la tecnología, los investigadores determinaron que la encriptación de 64 bits era muy fácil de decodificar.

WEP de 128 bits:

Debido a las deficiencias potenciales de seguridad de WEP de 64 bits, se desarrolló un método de encriptación más seguro de 128 bits. La encriptación de 128 bits incluye un largo de clave de 104 bits, más 24 bits adicionales de datos generados por el sistema (128 bits en total). Algunos fabricantes de hardware se refieren a la encriptación de 128 bits por el nombre de encriptación de 104 bits.

2.6.4 VPN (Virtual Private Network)

Una VPN (Red Privada Virtual) emplea tecnologías para crear un canal virtual privado sobre una red de uso público por lo que las VPN resultan ser una opción atractiva para proteger redes inalámbricas ya que funcionan sobre cualquier hardware inalámbrico y superan las limitaciones que tiene WEP.

Al utilizar VPN para configurar una red inalámbrica se debe asumir que la red inalámbrica es una red abierta e insegura, es decir, que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador o agrupando todos los puertos de acceso inalámbrico en una VLAN si se utiliza switching

Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

En el siguiente gráfico se muestra la estructura de una VPN para acceso inalámbrico seguro.

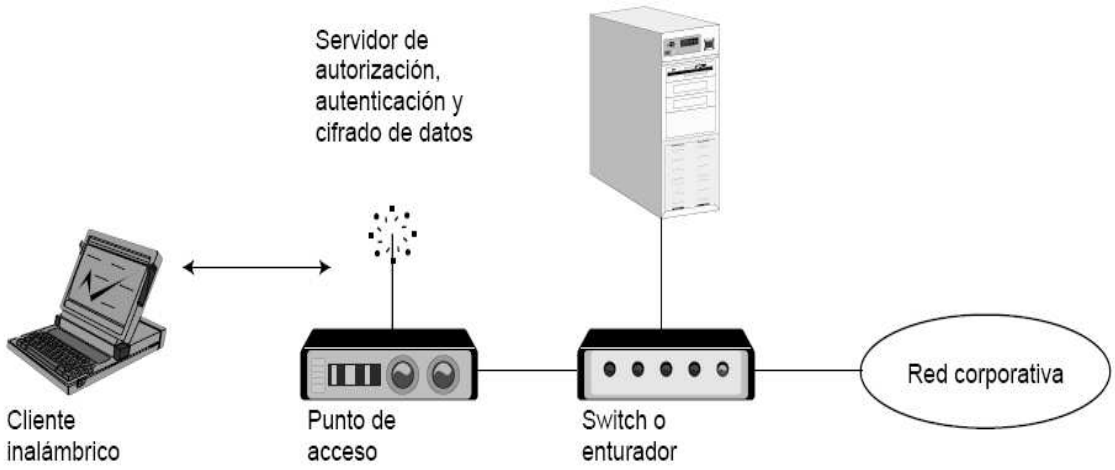


Figura 2.14. Estructura de una VPN para acceso inalámbrico seguro.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

2.6.5 802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red 802.11. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x. El protocolo 802.1x involucra tres participantes:

- El cliente, que desea conectarse con la red.
- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red.
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto) que recibe la conexión del suplicante. El autenticador actúa como Intermediario entre el cliente y el servidor de autenticación, y solamente permite el acceso a la red cuando el servidor de autenticación así lo autoriza.

El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red o logra enlazarse con un punto de acceso. En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal. La estación de trabajo envía un mensaje autenticador, indicando que desea iniciar el proceso de autenticación. El autenticador solicita a la estación que se identifique, mediante un mensaje. La estación se identifica mediante otro mensaje de respuesta.

Una vez recibida la información de identidad, el autenticador envía un mensaje de acceso al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.

El servidor de autenticación responde con un mensaje en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para

lograr el acceso, dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada.

Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.

2.6.6 WPA (Wi-Fi Protected Access)

WPA, acceso protegido Wi-Fi, es un estándar que mejora la protección WEP, mejorando el cifrado de los datos y brindando un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IV´s, con respecto a WEP. El mecanismo de autenticación usado en WPA emplea 802.1x, que fueron discutidos en la sección anterior. Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
- Modalidad de red casera, o PSK (Pre-Shared Key): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las

contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

2.7 COMPONENTES DE LAS WLAN´s

Para crear una red WLAN Wi-Fi, existen fundamentalmente seis tipos de componentes que permiten la interoperabilidad de un usuario inalámbrico con la red. Estos componentes son:

- Modem/Routers ADSL.
- Wireless Routers (enrutadores inalámbricos).
- Access Point (Puntos de Acceso).
- Tarjetas de red inalámbricas.
- Antenas.
- Amplificadores de señal.

De cada uno de estos equipos existe una gran variedad de marcas y precios dependiendo de las características que tenga cada uno de ellos en lo referente a área de cobertura, tecnología que utiliza, velocidad de transmisión, etc.

2.7.1 Modem/Routers ADSL-Cable

El Modem/Router es el dispositivo más popular para implementar redes inalámbricas, especialmente para WLAN´s caceras, ya que reúne en un solo equipo un Modem ADSL o Cable y un router como punto de acceso inalámbrico. Mediante el Modem ADSL o Cable se puede acceder a un servicio de Internet de banda ancha por medio de un distribuidor autorizado de servicio y con el Router se puede configurar una LAN inalámbrica segura y administrar a los usuarios que pertenecen a la misma.

(SIGUIENTE HOJA)

Figura 2.15. Modem/Router Netgear

Características:

- Compatible con los estándares inalámbricos 802.11b y 802.11g IEEE.
- Conmutador Auto-Sensing integrado de 4 puertos a Ethernet con velocidad de 10/100Mbps.
- Compatible con cable módem y módem xDSL (IP dinámica, IP estática)
- Antena desmontable 2dBi.
- Conexión inalámbrica de alta velocidad de hasta 54 Mbps con repliegue automático.
- Privacidad equivalente con cables (WEP) de 64 a 128 bits con cable HEX o ASCII, WPA-PSK (Pre-shared Key).
- Soporta hasta 100 sesiones de transferencia VPN simultáneamente.
- Restricción de acceso a Internet utilizando palabras clave de URL y tipo de servicios.
- Compatible con DMZ y servidores virtuales (Port Forwarding).
- Firewall con Network Address Translation (NAT) y Stateful Packet Inspection (SPI) para protegerse contra ataques de DoS.
- Compatible con UPnP (Plug & Play universal).
- Alertas de correo electrónico y logs en tiempo real cuando se producen ataques o actividades de Internet no autorizadas.
- Compatible con enrutamiento estático y servicio DNS dinámico.
- Característica de servidor DHCP que ubica hasta 253 usuarios.
- Fácil configuración y mantenimiento remoto con navegador Web (HTTP).

- Gama de 35 a 100 metros en interior, de 100 a 300 metros en exteriores (dependiendo del entorno)

2.7.2 Wireless Routers

A diferencia de los Modem/Routers, los enrutadores inalámbricos no poseen incluido en su carcasa un Modem ADSL o Cable por lo que es necesario tener un Moden ADSL independiente para poder conectarlo al enrutador inalámbrico. El funcionamiento del enrutador es igual al de los Modem/Routers, Todo lo que se requiere es un navegador de Internet y un adaptador de red que soporte TCP/IP (el idioma estándar de Internet).

Normalmente cada unidad que sale al mercado incorpora un disco compacto con un asistente de instalación que no es más que una ayuda para que el proceso de instalación del router inalámbrico sea más fácil básico para personas que no están ligadas con esta tecnología, principalmente a usuarios caseros.

Figura 2.16. Wíreles Router Linksys

Se puede configurar las funciones básicas y avanzadas del enrutador fácilmente a través de un navegador de Internet sin tener que instalar software adicional a la computadora. No hay disquetes que instalar o guardar y lo mejor de todo es que puede hacer cambios y llevar a cabo las funciones de instalación desde cualquier computadora en la red de manera fácil y rápida.

De manera general los enrutadores inalámbricos incorporan un conmutador de red de 4 puertos integrados de 10/100 Mbps que permite que el router actúe como un switch permitiendo que las computadoras con tarjetas de red RJ45 se conecten a la red. Este conmutador tiene un detector automático para ajustarse a la velocidad de los dispositivos conectados, el conmutador puede transferir datos entre las computadoras e Internet simultáneamente sin interrumpir o consumir recursos. Dependiendo del fabricante, varía la cantidad de puertos LAN en cada equipo.

También proporcionan soporte para el protocolo de paso VPN por medio del cual, si se conecta a la red empresarial desde un lugar remoto, el enrutador permitirá que esa computadora equipada con una conexión VPN pase a través de él hacia la red de la empresa, oficina u hogar.

Los routers inalámbricos poseen un servidor de DHCP (Protocolo de configuración del host dinámico) integrado que hace que la conexión sea más sencilla ya que este servidor asignará direcciones IP automáticamente a cada una de las computadoras enganchadas al router.

2.7.3 Access Points

Los Access Points son dispositivos que actúan como un switchs o concentradores inalámbricos que se encargan de recibir y enviar la información, por medio de ondas de radio, a los dispositivos de los usuarios que se encuentren presentes en la red. Pueden ser configurados para trabajar en modo Bridge (puente) y repetidor, al igual que los equipos anteriores, es configurable por medio de un browser y cuentan con todos los servicios de seguridad que fueron expuestos anteriormente.

Los access points normalmente tienen un puerto LAN de 10/100 Mbps para poder conectar un switch de ser necesario para añadir computadoras con tarjetas de red cableadas y dependiendo del modelo y marca el número de puertos puede

variar. A continuación se muestra una ilustración de un access point de la marca D-Link:

Figura 2.17. Access Point D-Link

Las características principales de los access points son las siguientes:

- Proporciona seguridad con WEP y WPA de 64 o 128 bits.
- Compatible con autentificación 802.1x y control de dirección para acceso de autorización de MAC.
- Compatible con la mayoría de sistemas operativos, como Windows 95/98/ME/NT/2000/XP, Unix y Mac.
- Permite a los usuarios desactivar la transmisión SSID para mejorar la seguridad inalámbrica.
- Un puerto Fast Ethernet Auto-Sensing integrado a 10/100Mbps.
- Escala de valoración de datos dinámicos a 54, 48, 36, 24, 18, 12, 9 y 6 Mbps para 802.11g. y escala de valoración de datos dinámicos a 11,5.5, 2 y 1 Mbps para 802.11b.
- Antena de diversidad desmontable de 2dBi Reemplazable por una antena de ganancia elevada opcional para ampliar el área de gama o cobertura.
- Fácil configuración y mantenimiento con navegador Web (HTTP).
- Distancia de la cobertura, de 50 a 100 metros en interiores y de 100 a 300 metros en exteriores dependiendo del entorno.

2.7.4 Tarjetas de red Inalámbricas

Estos dispositivos se encuentran en cada máquina que se va a conectar a la red inalámbrica normalmente vienen incorporados en las computadoras portátiles modernas. Para computadoras que no cuentan con este tipo tarjetas existen tarjetas externas que pueden ser conectadas mediante un conector PCMCIA o USB si son equipos portátiles o en un slot PCI si es un computador de sobremesa.

Estas tarjetas substituyen a las tarjetas de red Ethernet o Token Ring que se usan para redes cableadas y la velocidad de transmisión y recepción de los mismos es variable dependiendo del fabricante y del estándar que esté utilizando. A continuación se muestran los tipos de tarjetas de red comúnmente utilizadas en las redes WLAN:

Tarjetas Inalámbricas PCMCIA:

Permiten a usuarios de computadoras portátiles obtener libertad móvil para conectarse a la red inalámbrica del hogar o la oficina. Cumplen con el estándar IEEE 802.11g, haciéndola compatible en retroceso con las redes 802.11b.

Figura 2.18. Tarjeta PCMCIA Belkin

Figura 2.19. Adaptador PCMCIA

Adaptadores Inalámbricos PCMCIA a PCI:

Es un adaptador de tarjeta PCMCIA a PCI que se conecta en un slot de las computadoras de escritorio. Es compatible con el Standard 802.11g y el 802.11b.

Adaptadores Inalámbricos USB 2.0:
Estos dispositivos reúnen la conveniencia de USB 2.0 y la alta velocidad de 802.11g, permitiéndole conectarse fácilmente a la red a velocidades de hasta 54Mbps. La interfaz del USB 2.0 facilita una instalación Plug-and-Play sin problema alguno.

Figura 2.20. Adaptador Wireless USB

Figura 2.21. Tarjeta PCI 54 Mbps.

Adaptador PCI Inalámbrico de 54Mbps:
Cumple con el estándar IEEE 802.11g, haciéndola compatible en retroceso con las redes 802.11b para tener una compatibilidad asegurada mientras se navega en la red.

Las características de funcionamiento de estos dispositivos son similares entre si, a continuación se enlistan las características generales que tienen las tarjetas de red inalámbricas:

- Utiliza la banda de frecuencia de 2.4 GHZ la cual cumple con requisitos mundiales.
- Respalda a dispositivos inalámbricos IEEE 802.11g o 802.11b (11Mbps).
- Cambio dinámico de velocidad de datos a 54, 48, 36, 24, 18, 12, 9 y 6 Mbps para 802.11g.
- Cambio dinámico de velocidad de datos a 11, 5.5, 2 y 1Mbps para 802.11b.
- Soporta al modo Ad-Hoc y modo de infraestructura.
- Compatible con Windows 98(SE)/ME/2000/XP.
- Soportan 64/128/256-bit Protocolo de seguridad (WEP) y Claves especiales

- Soportan Wi-Fi con Acceso Protegido (WPA-PSK).
- Interferencia baja y la alta susceptibilidad garantizan un funcionamiento confiable.
- Antena dual integrada de la diversidad de la microcinta para el ambiente multidireccional.
- Cobertura de Distancia en el interior de 35 a 100 metros, exterior de 100~300 metros (dependiendo del ambiente).
- Montaje de Usuario sencillo y Utilidades de Diagnósticos.

2.7.5 Antenas

Las antenas son dispositivos que sirven para transmitir y recibir ondas de radio. Convierten la onda guiada por la línea de transmisión (el cable o guía de onda) en ondas electromagnéticas que se pueden transmitir por el espacio libre. Existen antenas de distintos tipos pero todas cumplen la misma misión: servir de emisor/receptor de una señal de radio.

La característica más importante de una antena es la ganancia. Esto viene a ser la potencia de amplificación de la señal. La ganancia representa la relación entre la intensidad de campo que produce una antena en un punto determinado, y la intensidad de campo que produce una antena omnidireccional (llamada isotrópica), en el mismo punto y en las mismas condiciones. Cuanto mayor es la ganancia, mejor es la antena.

Existen tres tipos de antenas que son: unidireccionales, bidireccionales y omnidireccionales y cada uno de estos tipos de antenas tienen un patrón de radiación definido.

Antenas Unidireccionales:

Las antenas Unidireccionales o Direccionales son las mejores en una conexión Punto-a-Punto, acoplamientos entre los edificios, o para los Clientes de una Antena Omnidireccional.

Las antenas direccionales (o yagui), tienen forma de tubo en cuyo interior tienen unas barras de metal que cruzan las cuales proporcionan las ganancias deseadas.

Figura 2.22. Antena unidireccional

La señal que emiten proporciona una ganancia que oscila entre los 15 y los 21 dBi. Hay que enfocarla directamente al lugar con el que se quiere enlazar. Como todas las antenas exteriores hay que protegerla ante posibles descargas eléctricas.

Antenas Bidireccionales:

Las antenas Bidireccionales son particularmente buenas en los pasillos o para corredores de edificios ya que radia o recibe la mayor parte de su energía en sólo dos direcciones

Figura 2.23. Antena Bidireccional

Antena Bidireccional de doble banda

La antena bidireccional de doble banda se la puede utilizar con los puntos de acceso administrados para LAN inalámbrica con antenas extraíbles para cubrir las transmisiones en grandes vestíbulos y pasillos existentes en el interior de los edificios empresariales.

(SIGUIENTE HOJA)

Figura 2.24. Antena Bidireccional de doble banda 3Com

Antenas Omnidireccionales:

Las antenas Omnidireccionales son buenas para cubrir áreas grandes, en la cual la radiación trata de ser pareja para todos lados es decir cubre 360º

Se utilizan principalmente para emitir la señal en todas las direcciones. En realidad el patrón de radiación en el plano horizontal es en forma de óvalo, y sólo emite en plano (no hacia arriba ni hacia abajo).

Figura 2.25. Señal emitida de antena Omnidireccional

Se suelen colocar en espacios abiertos para emisión en todas las direcciones. También se usan en espacios cerrados. Son fáciles de instalar y se fabrican con ganancias de hasta 15 dBi.

En la actualidad se ofrecen una amplia selección de antenas específicamente diseñadas para optimizar la conectividad 802.11 en diferentes

entornos. Estas antenas amplían el área de cobertura de los bridges para LAN inalámbrica y de los puntos de acceso con antenas desmontables. A continuación se muestra algunas antenas con sus características.

Antena Omnidireccional de doble banda:

Este tipo de antenas son idóneas para conexiones punto a multipunto de medio alcance con bridges de interiores entre edificios. Permite también ampliar el área de cobertura de puntos de acceso empresariales con antenas extraíbles. Trabajan en las dos bandas asignadas para WiFi (2.4 GHz y 5 GHz) Sus características básicas son:

- Ganancia de 2.4 GHz: 6 dBi.
- Ganancia de 5 GHz: 8 dBi.
- Tipo de conector: N hembra.
- Resistencia al viento: 125 mph.
- Diámetro de la base de montaje: 3,18 cm (1,2").

Figura 2.26. Antena Omnidireccional de doble banda

2.7.6 Amplificadores de señal

Los amplificadores de señal son de gran utilidad cuando no se está alcanzando suficiente cobertura y distancia con los equipos WLAN. Si nos encontramos en un ambiente complejo con muchos obstáculos como paredes, muebles, vidrios, estructuras metálicas etc., seguramente los equipos WLAN no

soportan el requerimiento de cobertura necesario para todas las aplicaciones de red. Normalmente existen tres opciones para resolver este problema:

- **Utilizar una mejor antena:** las antenas con mayor ganancia incrementan la distancia de la señal inalámbrica, pero a expensas del ángulo de cobertura horizontal. Estas en realidad no incrementan el nivel de la señal sino que más bien concentran su potencia en cierta dirección. Esto significa que se tiene como resultado menos ángulo de cobertura.
- **Utilizar la función de WDS para repetir:** la función WDS (Wireless Distribution System) permite que el access point repita la señal a otro access point, incrementando así la distancia de cobertura. Sin embargo, la configuración de software involucrada es más complicada y requiere equipo adicional.
- **Utilizar un Amplificador de Señal o "Power Booster":** el amplificador incrementa la intensidad de la señal emitida mediante la amplificación eléctrica de la potencia RF (radio frecuencia) a un mayor nivel. De esta amanera incrementa la distancia sin comprometer el ángulo horizontal de cobertura.

Las siguientes imágenes representan dos amplificadores de señal, una específicamente para 802.11b y otro para 802.11g cada uno con sus respectivas características.

Amplificador 802.11b

- Compatible con dispositivos inalámbricos WLAN 802.11b a una frecuencia de 2.4 GHz.
- Modelos de 20dBm (100mW), 23dBm (200mW) y 27dBm (500mW).
- Funcionamiento Bidireccional, half-duplex, auto-conmutacion vía detección de portadora.
- Ganancia transmitida: 12dB (Ajustable).
- Ganancia recibida: 14dB (Típica)

Figura 2.27. Amplificador 802.11b

Amplificador 802.11g

- Compatible con dispositivos inalámbricos LAN 802.11b u 802.11g, es decir, funciona en las 2 bandas de frecuencias Wi-Fi.
- Se compone de un pre-amplificador receptor de señales bajas y un poderoso amplificador trasmisor.
- Funcionamiento bidireccional, half duplex, auto-conmutacion vía detección de portadora.
- Modelos de 20dBm (100mW), 23dBm (200mW), 27dBm (500mW) y 30dBm (1W).
- Ganancia transmitida: 10dB (Adjustable)
- Ganancia recibida: 14dB (Typical)

Figura 2.28. Amplificador 802.11g

2.8 BANDAS DE FRECUENCIAS PARA WLAN

Para poder operar en todo el mundo con LAN´s inalámbricas se necesita una banda de frecuencia abierta a cualquier sistema de radio independientemente del lugar de donde se encuentre la red o los dispositivos inalámbricos. Para esto existen dos bandas de frecuencias abiertas que son:

- Banda ISM
- Banda UNII

2.8.1 Banda ISM

La banda ISM (Industrial Scientific and Medical) es una banda reconocida internacionalmente para las LAN de radio que opera en los siguientes rangos: 902 a 928 MHz. y 2.400 a 2.473 GHz.

Estas bandas de frecuencia, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales pero en la actualidad se encuentran abiertas para equipos inalámbricos como teléfonos, accesorios para redes WLAN, WWAN, etc.

El ancho de banda total de la banda ISM es de 73 MHz. y consta de 11 canales asignados. El concepto de canal es similar al del canal de televisión: representa una banda de frecuencias a través de la cual se envía o se recibe información. No todos los países admiten todos los canales de la banda ISM. En Europa se admiten 13 canales ISM. En la siguiente tabla se presentan las frecuencias asignadas a cada canal.

CANAL	*FREC. BAJA*	*FREC.CENTRAL*	*FREC. ALTA*
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438

5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473

Tabla 2.3. Canales de la banda ISM

A la hora de configurar una red inalámbrica con varias estaciones base, es fundamental seleccionar el canal adecuado para cada estación base. De lo contrario, esto puede perjudicar el rendimiento de la red (tráfico más lento).

2.8.2 Banda UNII

La banda de 5 GHz UNII (Unlicensed National Information Infrastructure) es la otra banda de frecuencias en la que trabaja WIFI. La banda de 5 GHz está formada por tres sub-bandas, UNII-1 (5.15 – 5.25 GHz), UNII-2 (5.25 – 5.35 GHz) y UNII-3 (5.725 – 5.825 GHz). Cuando se utilizan tanto UNII-1 como UNII-2, hay 8 canales sin solapamiento disponibles. El ancho de banda total disponible en la banda de 5 GHz también es mayor que en la banda de 2,4 GHz (300 MHz por 73 MHz). Así pues, una WLAN basada en el 802.11a puede admitir un mayor número de usuarios de alta velocidad simultáneos sin peligro de que surjan conflictos. Un inconveniente de utilizar la banda de 5 GHz es que las frecuencias utilizadas no están estandarizadas internacionalmente.

El alcance de las señales de radio varía con la frecuencia. En general, las frecuencias más bajas atraviesan los obstáculos más fácilmente, con lo cual su tendencia es a llegar a sitios más lejanos. En contraste, las altas frecuencias son más fácilmente reflejadas por muros o edificios.

Los organismos de estandarización internacionales establecen las normativas con detalle para asegurar que las tecnologías inalámbricas no tengan

consecuencias negativas sobre los diversos sistemas que utilizan tecnología de radiofrecuencia (RF). Los productos WLAN cumplen con estos estándares de seguridad y con las normativas de compatibilidad electromagnética (EMC).

2.9 INTERFERENCIA Y ATENUACIÓN

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por la acción de materiales ambientales. La inspección en el lugar nos ayudará a identificar los elementos que afecten en forma negativa a la señal. En la siguiente tabla, se enumeran los materiales nocivos que se deben considerar con el propósito de realizar una instalación de equipos inalámbricos.

MATERIAL	***INTERFERENCIA***	***EJEMPLO***
Madera	Baja	Escritorios, mesas, puertas
Vidrio	Baja	Ventanas, vitrinas, puertas
Amianto (fibras minerales)	Baja	Techos
Yeso	Baja	Paredes Interiores
Ladrillo	Media	Paredes interiores y exteriores
Hojas	Media	Árboles y plantas
Cerámica	Alta	Tejas, figuras
Vidrio (plomo)	Alta	Ventanas
Metales	Muy Altas	Vigas, armarios

Tabla 2.4. Materiales que provocan interferencia en las señales inalámbricas

Ya que las redes inalámbricas operan en un espectro de frecuencias utilizado comúnmente por otras tecnologías, pueden encontrarse interferencias que influyan negativamente en el rendimiento de nuestra red. Las siguientes son algunas de las tecnologías que más frecuentemente encontraremos en el hogar o en la oficina, y que pueden causar inconvenientes:

• Bluetooth
• Hornos microondas
• Algunos teléfonos inalámbricos (los que operan en 2,4 GHz o más)
• Otras redes WLAN

2.9.1 Atenuaciones por solapamiento de la señal

Los efectos multitrayectoria describen el fenómeno en el cual una señal de radio frecuencia toma varios caminos para llegar hasta el receptor en diferentes tiempos. Este efecto se produce al momento en que la señal de radio se refleja o rebota varias veces en un objeto.

Al momento que llegan las señales al receptor éstas se solapan en tiempos diferidos causando interferencias y debilitando su potencia entre si mismas. El peor caso del solapamiento se extiende la fase entre dos señales por 180 grados (pudiendo incluirse también atenuaciones por obstáculos) por la diferencias de tiempo, haciendo que las señales se eliminen en su totalidad.

Es por esto que puede ocurrir el caso en que no se consiga una conexión WLAN aunque una computadora y un access point se encuentren en la misma oficina y a unos pocos metros de distancia entre ellos. El efecto multitrayectoria se puede esquematizar de la siguiente manera:

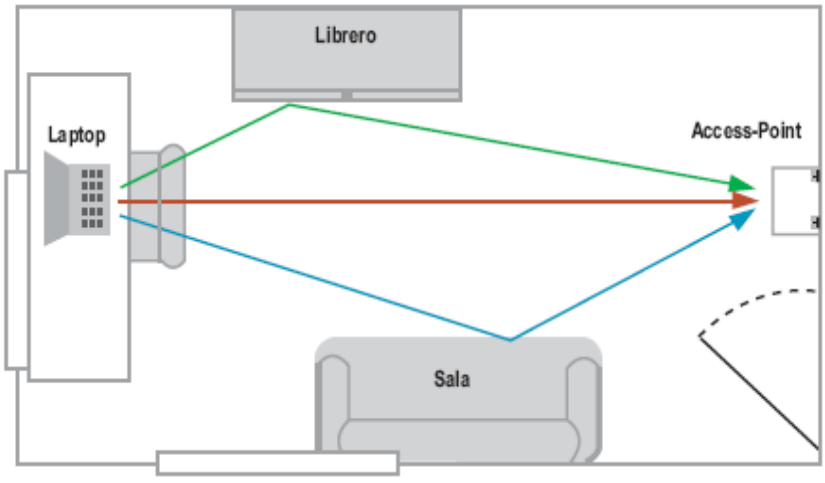


Figura 2.29. Efecto multitrayectoria

2.10 MODELO DE CAPAS 802.11

El estándar 802.11 hace referencia al modelo OSI (Open Systems Interconnection) desarrollado por la Organización Internacional de Estandarización (ISO), el cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red. El estándar Wi-fi 802.11 trabaja en las dos capas inferiores del modelo OSI que son la capa física y la capa de enlace como indica la figura.

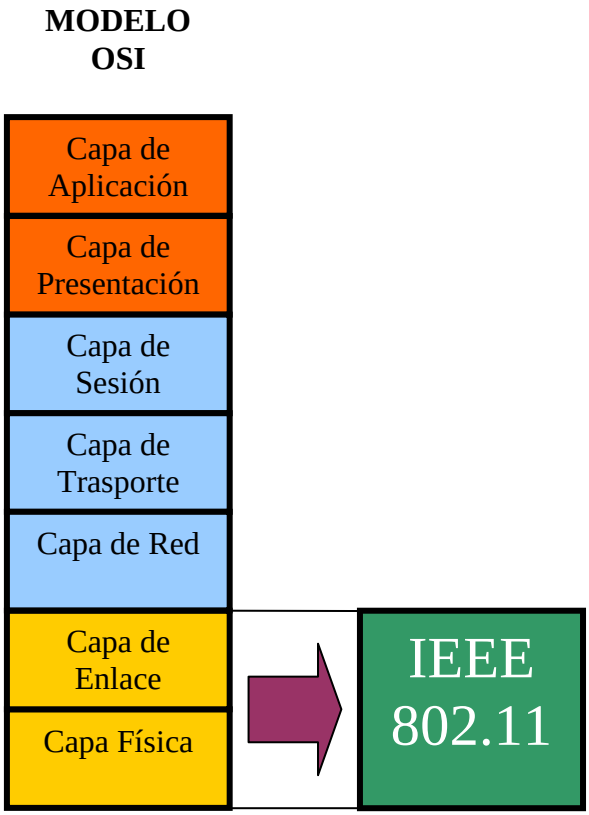


Figura 2.30. Modelo OSI y IEEE 802.11

Los dos estándares para redes LAN y WLAN que trabajan en las capas Física y de enlace de datos son el estándar 802.11 y el estándar 802.2. Como se ha indicado en este trabajo el estándar 802.11 es descrito para las redes inalámbricas de área local mientras que el estándar 802.2 es descrito de manera general para las redes LAN y se encarga de realizar el *control de enlace lógico,* es decir, trabaja en la capa 2 del modelo OSI como indica la figura.

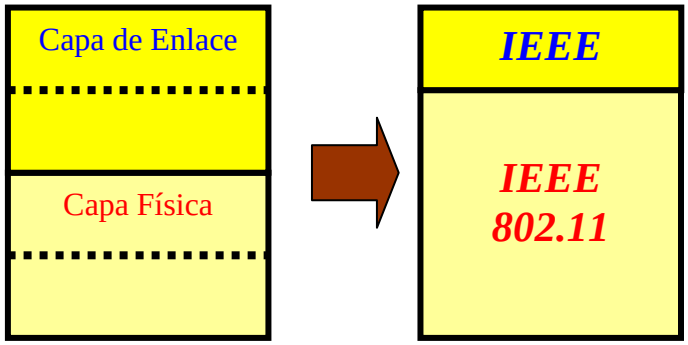


Figura 2.31. Modelo OSI, IEEE 802.11 e IEEE 802.2

Este gráfico indica que la capa de enlace de datos es dividida en subcapas, al igual que la capa física las cuales trabajan con 802.11 y 802.2 como se va a explicar para cada capa más detalladamente a continuación.

2.10.1 Capa Física

La capa física describe las características físicas de la comunicación, es decir, es la que se encarga de la modulación y la codificación de las señales, los códigos de canales, potencias de transmisión, longitudes de onda, sincronización, temporización y distancias máximas, etc. El gráfico muestra un esquema de la capa física.

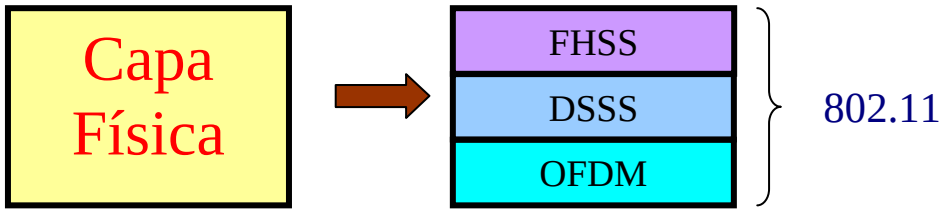


Figura 2.32. Capa Física 802.11

El estándar 802.11 define varios métodos y tecnologías de transmisión para implantaciones de LAN inalámbricas que son:

- Espectro ensanchado por saltos de frecuencia de (FHSS)

- Espectro ensanchado de secuencia directa (DSSS)
- Modulación por división de frecuencias ortogonales (OFDM)

Espectro Ensanchado (Spread Spectrum)

La tecnología de espectro ensanchado es usada en la transmisión de datos digitales sobre canales de comunicación que pueden ser corrompidos por interferencias o canales que pueden ser utilizados por otros usuarios o aplicaciones. Spread spectrum es una técnica que ha sido generada y ampliamente utilizada en el sector de la defensa por sus excelentes propiedades en cuanto a inmunidad a interferencias y a sus posibilidades de encriptación.

Los principales elementos que intervienen en una comunicación de espectro ensanchado son los moduladores y los generadores de secuencia pseudo-aleatorias. El diagrama de bloques que se muestra en la figura ilustra los elementos básicos de un sistema comunicación digital basada en spread spectrum.

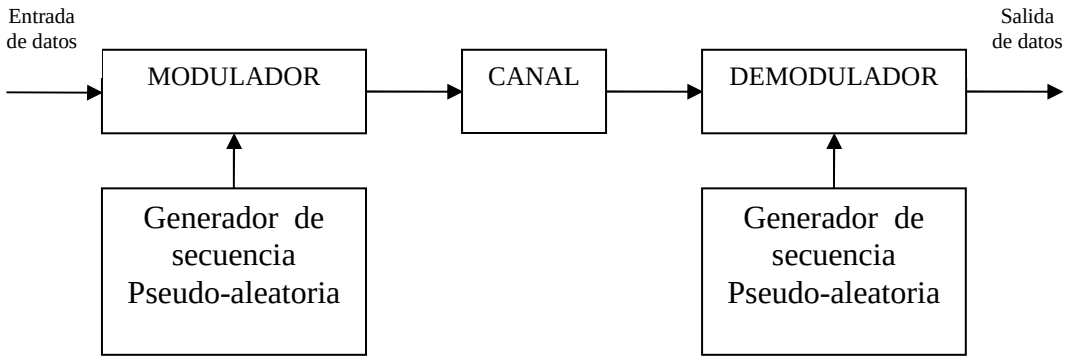


Figura 2.33. Sistema básico de comunicación digital Spread Spectrum

El objetivo de la tecnología de espectro ensanchado es difundir la señal de información a lo largo del ancho de banda disponible, es decir, en vez de concentrar la energía de las señales alrededor de una portadora concreta se la reparte por toda la banda disponible.

El ancho de banda es mayor de lo que se necesita estrictamente para la transmisión de la información y ésta mayor amplitud de banda puede obtenerse de dos maneras: por salto de frecuencia (FHSS) y por secuencia directa (DSSS).

FHSS ("Frequency Hopping Spread Spectrum")

Fue la primera implementación de Espectro Amplio y funciona de la siguiente manera: Los datos son divididos en paquetes de información, solo que estos paquetes son enviados a través de varias frecuencias, esto es conocido como "Hopping Pattern", la intención de enviar la información por varias frecuencias es cuestión de seguridad, ya que si la información fuera enviada por una sola frecuencia sería muy fácil interceptarla. Además, para llevar acabo la transmisión de datos es necesario que tanto el aparato que envía como el que recibe información coordinen este denominado "Hopping Pattern". El estándar IEEE 802.11 utiliza FHSS, aunque hoy en día la tecnología que sobresale utilizando FHSS es Bluetooth

DSSS ("Direct Sequence Spread Spectrum")

DSSS no requiere enviar la información a través de varias frecuencias, la manera en que DSSS logra esto es mediante un transmisor; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos. Es precisamente el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 m.

OFDM

La modulación OFDM, (Ortogonal Frequency Division Multiplexing) es una técnica de modulación por división de frecuencia que permite transmitir grandes cantidades de datos digitales sobre una onda de radio. OFDM trabaja dividiendo el espectro disponible en múltiples subportadoras que son transmitidas simultáneamente hacia el receptor en diferentes frecuencias. OFDM reduce la diafonía (efecto de cruce de líneas) durante la transmisión de la señal.

2.10.2 Capa de Enlace de Datos

La capa de enlace es la que se encarga del flujo de la información sobre la red, es decir, asegura que la información enviada de un host conectado directamente a otro llegue libre de errores e indica el como son transportados los paquetes de datos sobre el nivel físico. Este nivel es dividido en dos subcapas: Control de enlace lógico (Logical Link Control) y Control de acceso al medio.

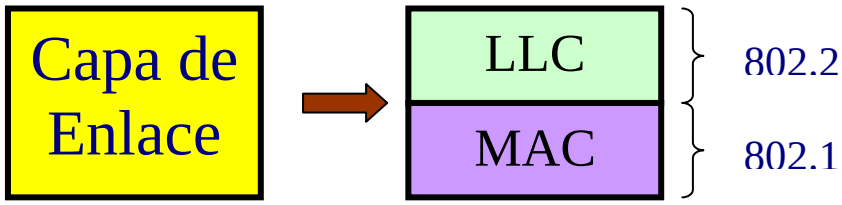


Figura 2.34. Capa de Enlace de Datos 802.11

Subcapa LLC (Logical Link Control)

La subcapa LLC se ubica en la parte superior de la capa de enlace y define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores. Las funciones de esta subcapa son:

- Encapsula el paquete entregado por la capa de red en forma de tramas (le añade un encabezado).
- Se ocupa de los errores de transmisión.
- Regula el flujo de las tramas (control de flujo).
- Administra la capa de enlaces (gestión).

Subcapa MAC (Media Access Control)

La subcapa MAC se encuentra en la parte inferior del la capa de enlace del modelo OSI. El algoritmo básico de acceso a este nivel es el llamado CSMA/CA, Acceso múltiple por detección de portadora con evasión de colisiones (Carrier Sense Multiple Access/Collision avoidance) y es utilizado para evitar colisiones entre los paquetes de datos en una red inalámbrica ya que estas redes no cuentan con un sistema practico para enviar y recibir paquetes simultáneamente. Este algoritmo funciona de la siguiente manera:

1. El primer paso es reconocer el estado del canal, es decir hacer un testeo del medio para determinar si se encuentra en estado libre u ocupado.
2. Si el testeo del canal indica que el medio esta desocupado (no se encuentra ninguna trama de datos en el canal), la estación ejecuta un tiempo de espera adicional llamada espaciado entre tramas IFS (Inter frame Spacing)
3. Si durante este intervalo temporal el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.
4. Una vez finaliza esta espera la estación ejecuta el llamado algoritmo de Backoff, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda (CW). El algoritmo de Backoff nos da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.
5. Mientras se ejecuta la espera marcada por el algoritmo de Back-off se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas.

El siguiente gráfico representa el diagrama de flujo del funcionamiento de CSMA/CA.

(SIGUIENTE HOJA)

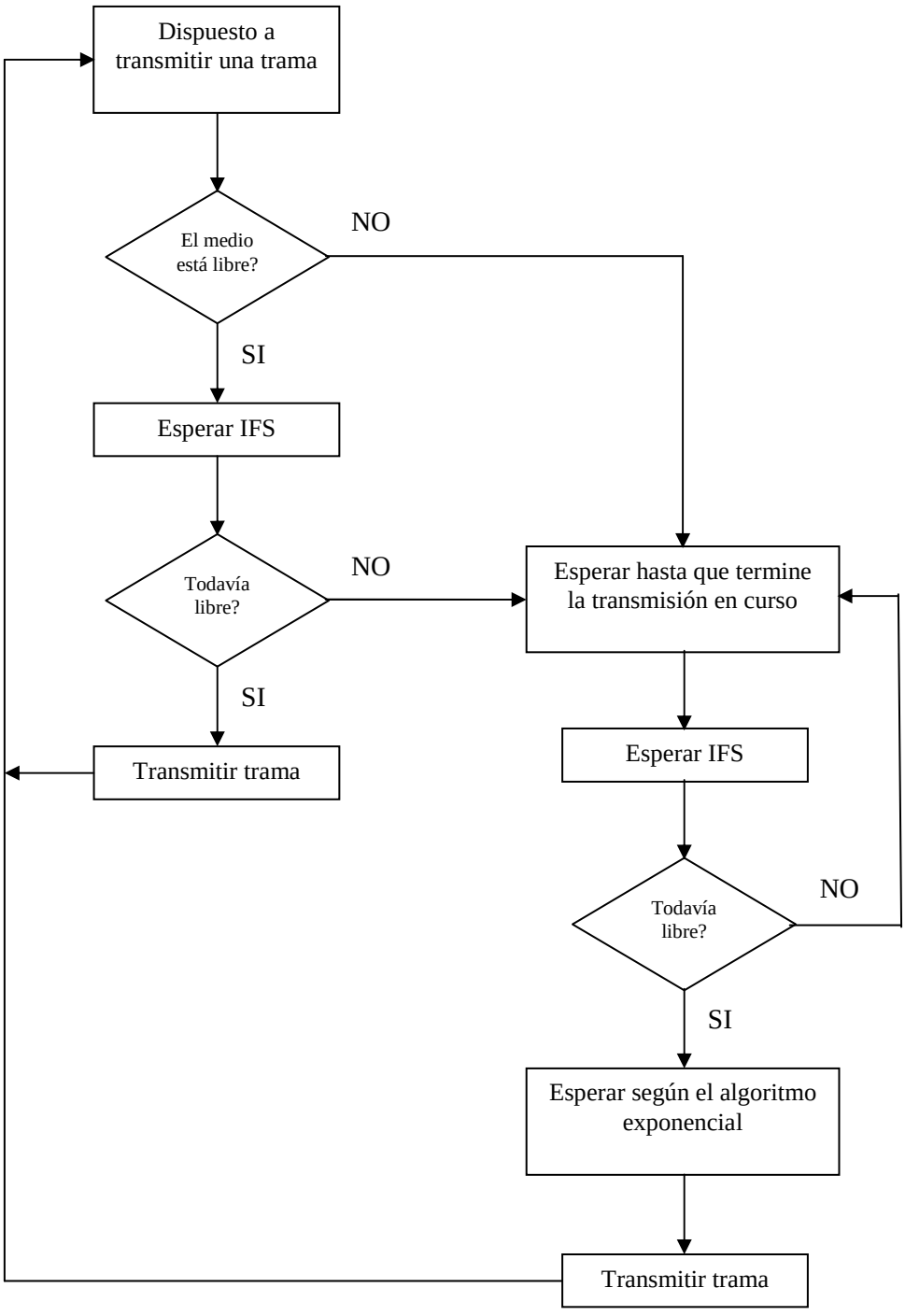


Figura 2.35. Diagrama de flujo CSMA/CA

CAPÍTULO III

DISEÑO DE LA RED INALÁMBRICA

El proyecto que se planteó para la Empresa Metropolitana de Obras Públicas de Quito tiene como objetivo específico analizar la factibilidad de sustituir su red cableada existente por una red inalámbrica para dar movilidad a los usuarios que necesitan desplazarse de un lugar a otro con su equipo de trabajo. Esta sustitución de la red es aplicable ya que muchos de los departamentos que existen en el edificio necesitan compartir información en reuniones que se efectúan en distintas oficinas del edificio, otorgando así una mayor flexibilidad al momento de realizar estos trabajos de cada empleado de la empresa.

El presente capítulo comprende el diseño de la red inalámbrica para el edificio de la EMOP-Q, el cual va a ser desarrollado mediante el análisis previo de los servicios de red que dispone actualmente el edificio para poder dimensionar los requerimientos que son necesarios para desarrollar una red WLAN, tomando en cuenta una alta dedicación en las mediciones de conectividad y los planos de cobertura necesarios para abarcar todo el espacio de trabajo del edificio.

3.1 CRITERIOS DE DISEÑO DE LA RED.

Una red inalámbrica de área local debe cumplir los siguientes puntos básicos para obtener un funcionamiento óptimo en la transmisión y recepción de información:

- Cobertura completa del área determinada.
- Capacidad suficiente para soportar el tráfico exigido por los usuarios.
- Fácil acceso y configuración.
- Alto nivel de seguridad.

- Mínima interferencia y pérdida de señal.

Estos requerimientos son cubiertos esencialmente por la correcta ubicación, instalación y configuración de los equipos inalámbricos y por la adecuada asignación de los canales de funcionamiento lo cual será desarrollado de una forma muy detallada mediante pruebas de cobertura y de conectividad.

Para diseños inalámbricos LAN no existen reglas simples de cálculo sino que es necesario hacer pruebas y mediciones. Hay que hacer pruebas exhaustivas y poner especial énfasis en aspectos de propagación de la señal y cobertura para los denominados “puntos muertos”, que son lugares en donde la señal inalámbrica tiene dificultad para llegar, para lograr cubrir el área de interés.

Al colocar los access points se deben espaciar lo máximo para asegurar una cobertura total del área. Este criterio ayuda a reducir las interferencias co-canal, costo de equipos e instalación. El gráfico que se muestra a continuación indica el volumen de cobertura “idealizada” para un access point con relación a los pisos superior e inferior del piso en el que se encuentra.

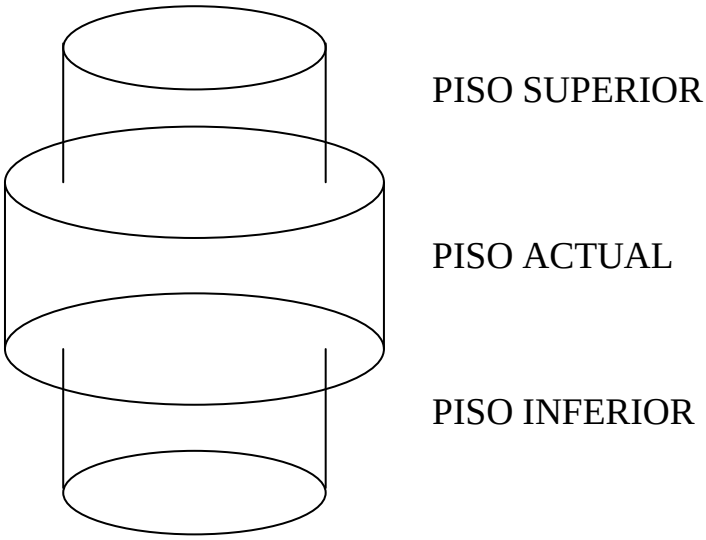


Figura 3.1. Cobertura idealizada para access points en diferentes pisos.

Al cambiar de ubicación un access point, todo el volumen se mueve. Si hay varios access points, el traslape debe ser mínimo para impedir la existencia de interferencia co-canal o de canal adyacente.

La asignación de canales para los access points debe ser efectuada según el número de access point que se vayan a utilizar tomando en cuenta los resultados de las pruebas y los mapas de cobertura que se los desarrollará más adelante. Para edificios con más de dos pisos es recomendable utilizar los canales 1, 4, 7 y 11 para evitar así la interferencia co-canal y la interferencia por canal adyacente.

En el siguiente gráfico se muestra una asignación básica de canales que se pueden ocupar cuando se utiliza más de un access point, para evitar problemas de comunicación por interferencia. Estos canales pueden variar según el diseño que se desee implementar.

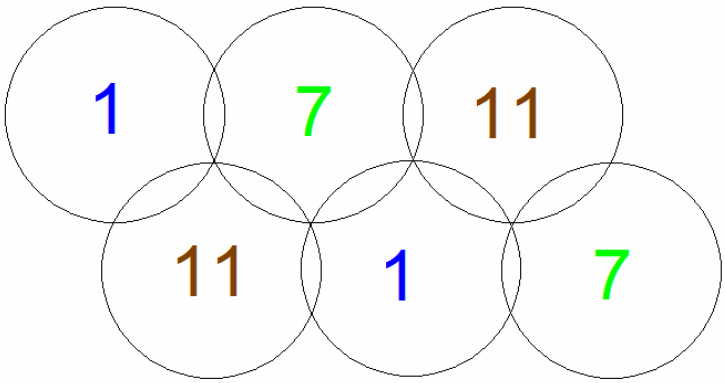


Figura 3.2. Asignación de canales sin interferencia.

La correcta configuración de las tarjetas de red es también un punto importante ya que deben ser configuradas con el canal asignado para el access point al cual se va a enganchar, caso contrario no se obtendría una buena recepción de señal y por ende no se podría conectar a la red con una potencia adecuada. Es necesario también, utilizar la mayor potencia de transmisión de cada tarjeta para evitar que las conexiones sean de un nivel de recepción bajo.

3.2 SITUACIÓN ACTUAL DE LA RED

3.2.1 Dimensionamiento del edificio

El edificio de la EMOP-Q tiene siete pisos. La planta baja y el primer piso tienen una extensión de 299 m^2. (29.9 metros de largo y 10 metros de ancho), del segundo al sexto piso tiene una extensión de 270 m^2. (27 metros de largo y 10 metros de ancho). La planta baja y el primer piso tienen estructura idéntica así como los pisos del segundo al sexto. En las siguientes figuras se indica el esquema estándar de los pisos y el área que ocupan las distintas oficinas de cada piso:

Figura 3.3. Modelo de Planta baja y primer piso.

Figura 3.4. Modelo del Segundo al sexto piso.

3.2.2 Distribución

El edificio tiene diferentes departamentos o unidades de trabajo que están distribuidos de la siguiente manera por cada piso:

Piso 0 (Planta baja):

- Atención al público
    - Recepción
    - Guardia
- Tesorería
    - Jefatura
    - Caja
- Comunicación Social
    - Jefatura
    - Secretaria
- Secretaria General
    - Jefatura
    - Secretaria
    - Recepción y tramite de documentos
- Archivo financiero
- Copiadora

Piso 1

- Unidad de Fiscalización
    - Jefatura
    - Secretaria
    - Archivo
    - Zona norte
    - Zona sur
    - Reajuste de precios
    - Supervisión zona norte
    - Supervisión zona sur
    - Sala de sesiones

Piso 2:

- Unidad Administrativa
    - Jefatura
    - Secretaria
    - Adquisiciones
    - Bienes
    - Jefatura de Bienes
    - Bodega de Bienes
    - Servicios Generales
- Unidad de Relaciones humanas
    - Jefatura
    - Secretaria
    - Remuneraciones
    - Servicio social y seguridad industrial
    - Capacitación
    - Archivo

Piso 3:

- Gerencia Técnica
    - Gerencia
    - Secretaria
- Unidad de Programación
    - Jefatura
    - Secretaria
    - Área técnica
- Unidad de Obras Públicas
    - Jefatura
    - Secretaria
    - Área técnica
- Unidad de Contrataciones
    - Jefatura
    - Secretaria
    - Supervisión Construcciones Mantenimiento
- Tecnología de Informática

  - Jefatura
  - Secretaria
  - Área técnica
  - Cuarto de equipos

Piso 4:

- Gerencia de Parques y Jardines
  - Gerencia
  - Secretaria
  - Diseños
  - Nomenclatura
- Unidad de estudios
  - Jefatura
  - Secretaria
  - Diseños
  - Estructuras
  - Archivos

Piso 5:

- Gerencia Administrativa Financiera
  - Jefatura Financiera
  - Secretaria
  - Gerencia
  - Área de contabilidad
  - Área de presupuesto
  - Contribución y mejoras

Piso 6:

- Gerencia General
  - Gerencia
  - Secretaria
  - Sala de sesiones
- Asesoría Jurídica

  - Asesor Jurídico
  - Secretaria
  - Expropiaciones
  - Contrataciones
- Desarrollo institucional y Tecnología de la Informática
  - Jefatura
  - Analistas
  - Secretaría

3.2.3 Materiales que componen el área de trabajo del edificio.

Uno de los puntos principales para realizar un diseño de red inalámbrica es identificar los materiales que componen el edificio para determinar que cantidad de pérdida de la señal existirá.

Como un edificio cualquiera, está construido con concreto y hierro, lo que produce gran atenuación hacia el exterior del edificio. Las divisiones de las oficinas en cada piso están hechas por paneles de madera que tienen una altura de 1.5 metros y en el cuarto piso estos paneles se extienden hasta el techo con vidrio delgado. La estructura de estos paneles está hecha de aluminio y las puertas de madera delgada. Aparte de esto, la mayoría de muebles son de madera (escritorios, anaqueles, archivadores, etc.).

Los niveles de atenuación de los materiales fueron indicados en la tabla 2.4 del capitulo II por lo que se puede indicar que los materiales existentes en el edificio son de interferencia media a excepción de el aluminio en los paneles de divisiones que son de interferencia alta pero como este aluminio se encuentra únicamente en los bordes y uniones de los paneles se puede tomar a este metal como un nivel de atenuación media.

En resumen, no existen elementos que puedan alterar la señal de los equipos inalámbricos de una forma significativa.

3.2.4 Esquema de la red actual

Este Esquema representa a la red actual del edificio de la EMOP-Q con la cantidad de puntos de red existentes en cada piso y con los tipos de servidores con los que cuenta esta infraestructura de red.

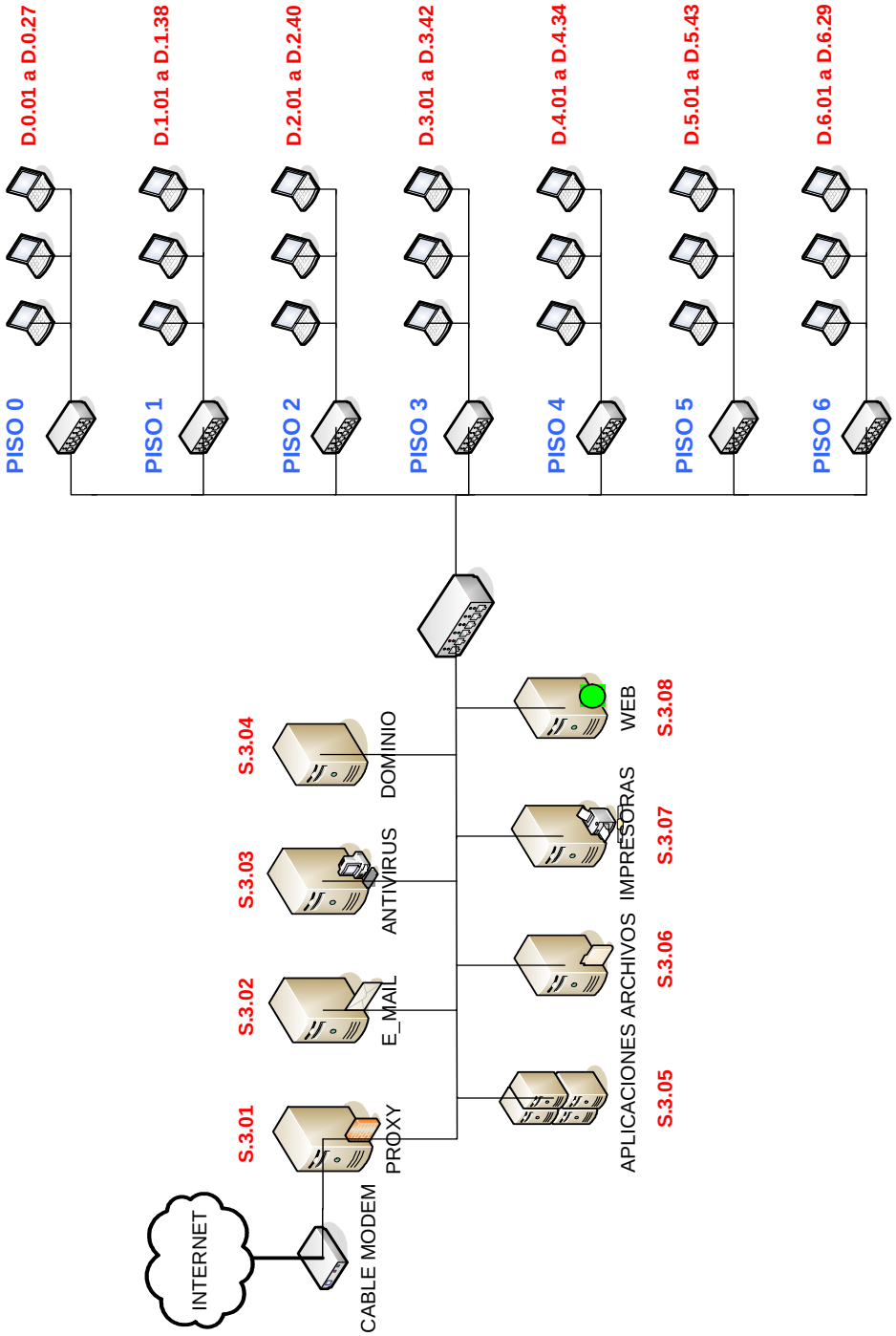


Figura 3.5. Esquema de la red actual.

3.2.5 Esquema de distribución física

En este esquema se presenta de manera general la conexión física de red que se encuentra en cada piso del edificio de la EMOP-Q.

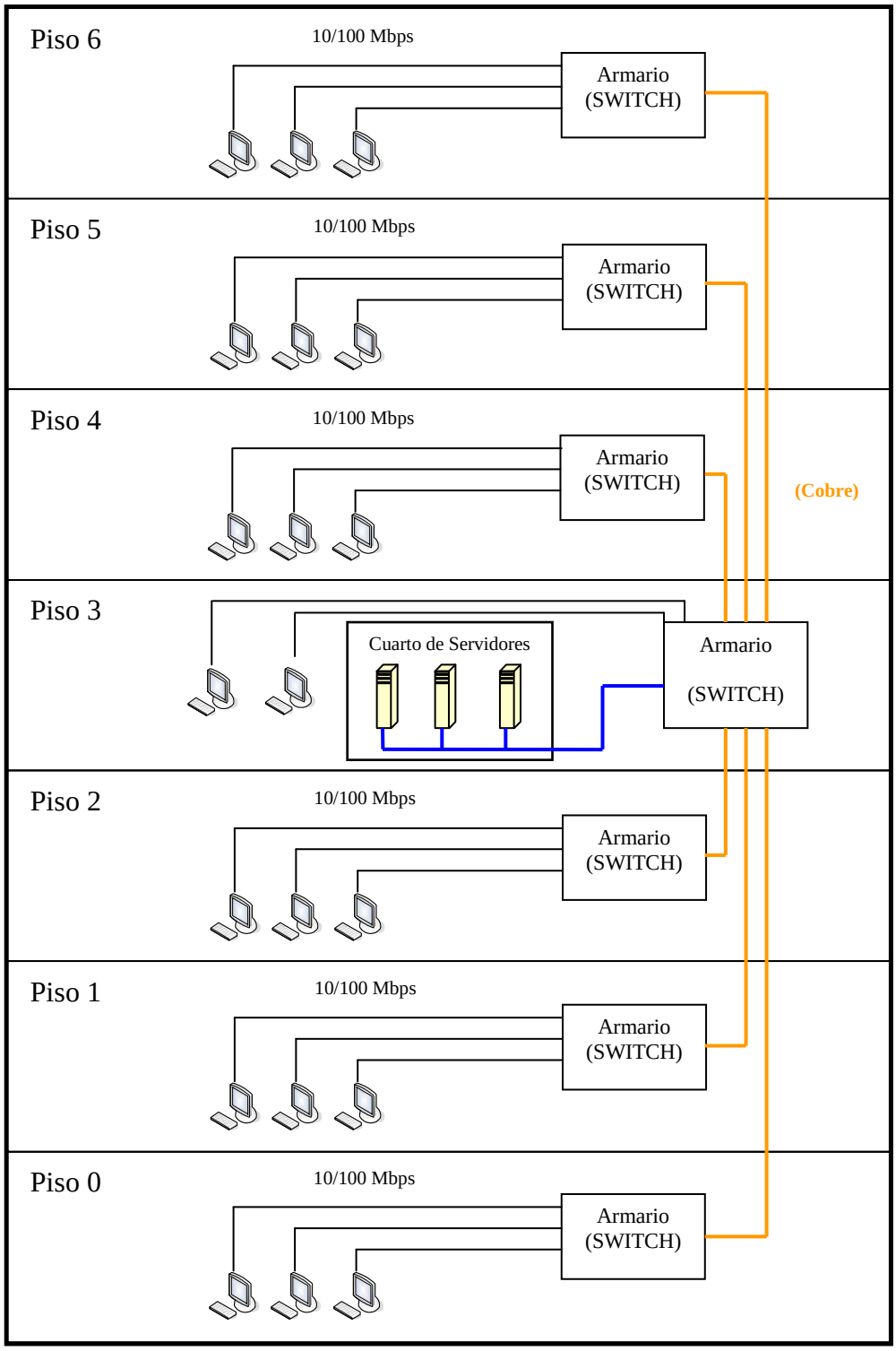


Figura 3.6. Esquema de distribución física.

3.2.6 Servicios de red que dispone la EMOP-Q:

Servicios Generales

- Control de acceso por Dominio
- Servicio de Internet – Intranet
    - Navegación Web
        - Control de acceso por usuario
        - Control de acceso por contenido
    - Web-mail
    - POP
- Compartir archivos
- Compartir dispositivos

Tipo de conexión a Internet, ancho de banda y proveedor:

- CABLE MODEM enlace dedicado de 512 kpbs.
  TVCABLE - SERVICIO PREMIUM

Servidores de red:

- Firewall + Proxy (Linux ES 4.0+ Squid)
- Servidor de Dominio (w2k Server)
- Servidor de Correo (Lotus Notes)
- Servidor Antivirus (Symantec Antivirus Corporate Edition)
- Servidores de Aplicaciones (Producción y Desarrollo)
    - SQL Server 2000 (w2k Server)
    - Oracle 10G (Linux ES 4.0)
- Servidor Web (Linux ES 4.0 + Apaches + PHP-UKE (Administrador de Contenido))
- Servidor de Impresoras (w2k Server)
- Servidor de Archivos (w2k Server)

3.3 DENSIDAD DE USUARIOS

3.3.1 Número de puntos de red y Host.

En el diseño se debe considerar la cantidad de usuarios que existe en cada piso, para esto tomamos en cuenta en primer lugar la cantidad de puntos de red que existen en cada piso y los host´s que están habilitados en los mismos obteniendo los siguientes datos en la siguiente tabla de resumen:

PISO	***Número de Puntos de red***	***Host´s Habilitados***
PB	27	23
1 (Mz)	38	36
2	40	32
3	42 más 8 servidores	32
4	34	29
5	43	36
6	29	22
Total	253 puntos de red	210 host´s habilitados

Tabla 3.1. Puntos de red y host´s habilitados en cada piso.

Se tiene una mayor concentración de tráfico en los pisos del 1 al 5 y menor tráfico en el piso 0 y 6 por lo que obtenemos un dato importante para ubicar los equipos.

3.3.2 Requerimientos de los usuarios

Al ser una empresa que se dedica a realizar proyectos de tipo civil o arquitectónico los servicios que requiere cada usuario son básicos, es decir, cada usuario del edificio necesita acceso a Internet de baja velocidad (es por eso que la empresa contrata un servicio de Internet de 512 Kbps), acceso al servidor de e_mail, al servidor web y servicio para compartir archivos y dispositivos.

3.4 PLANOS DEL EDIFICIO

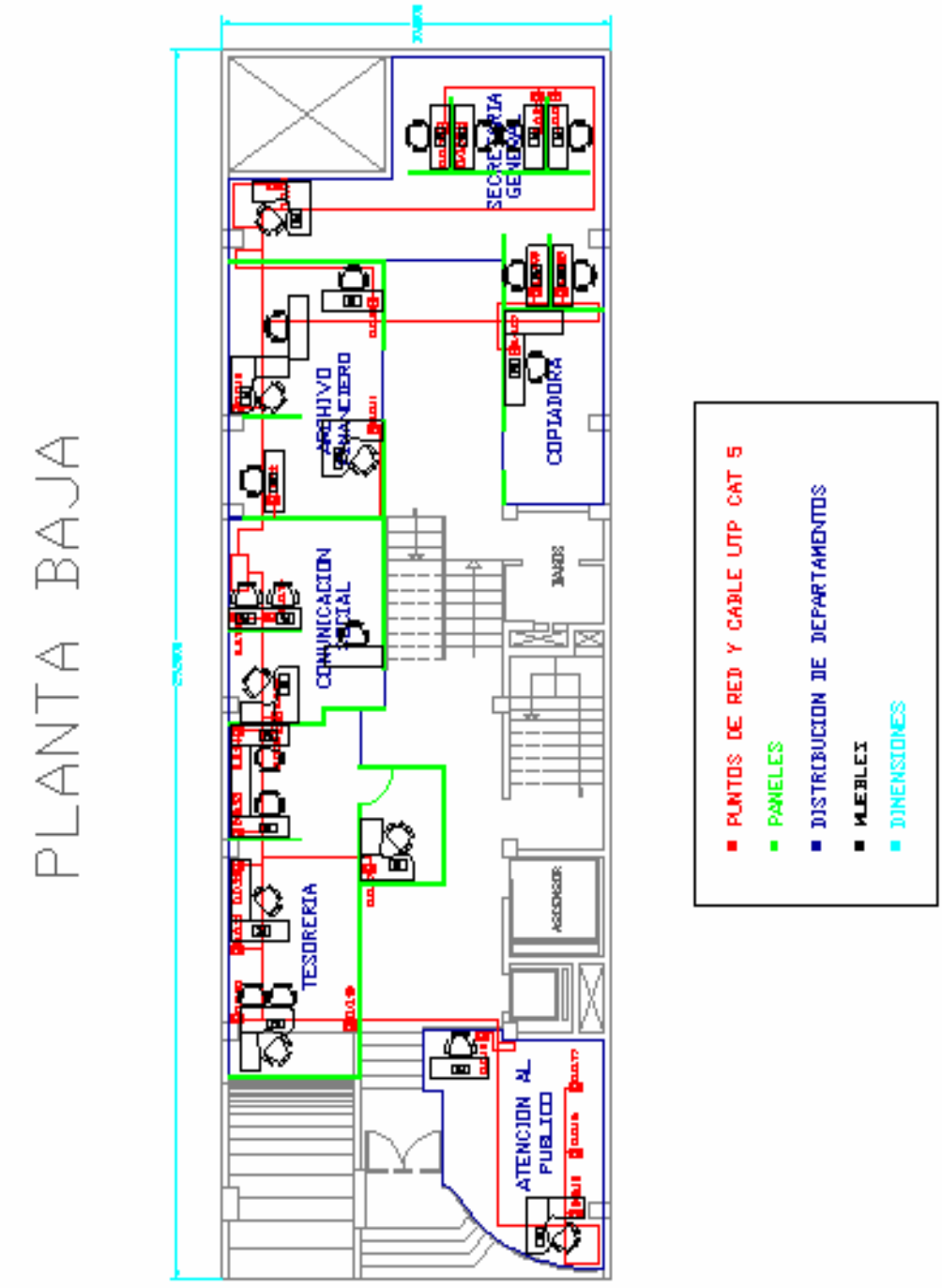


Figura 3.7. Planta Baja.

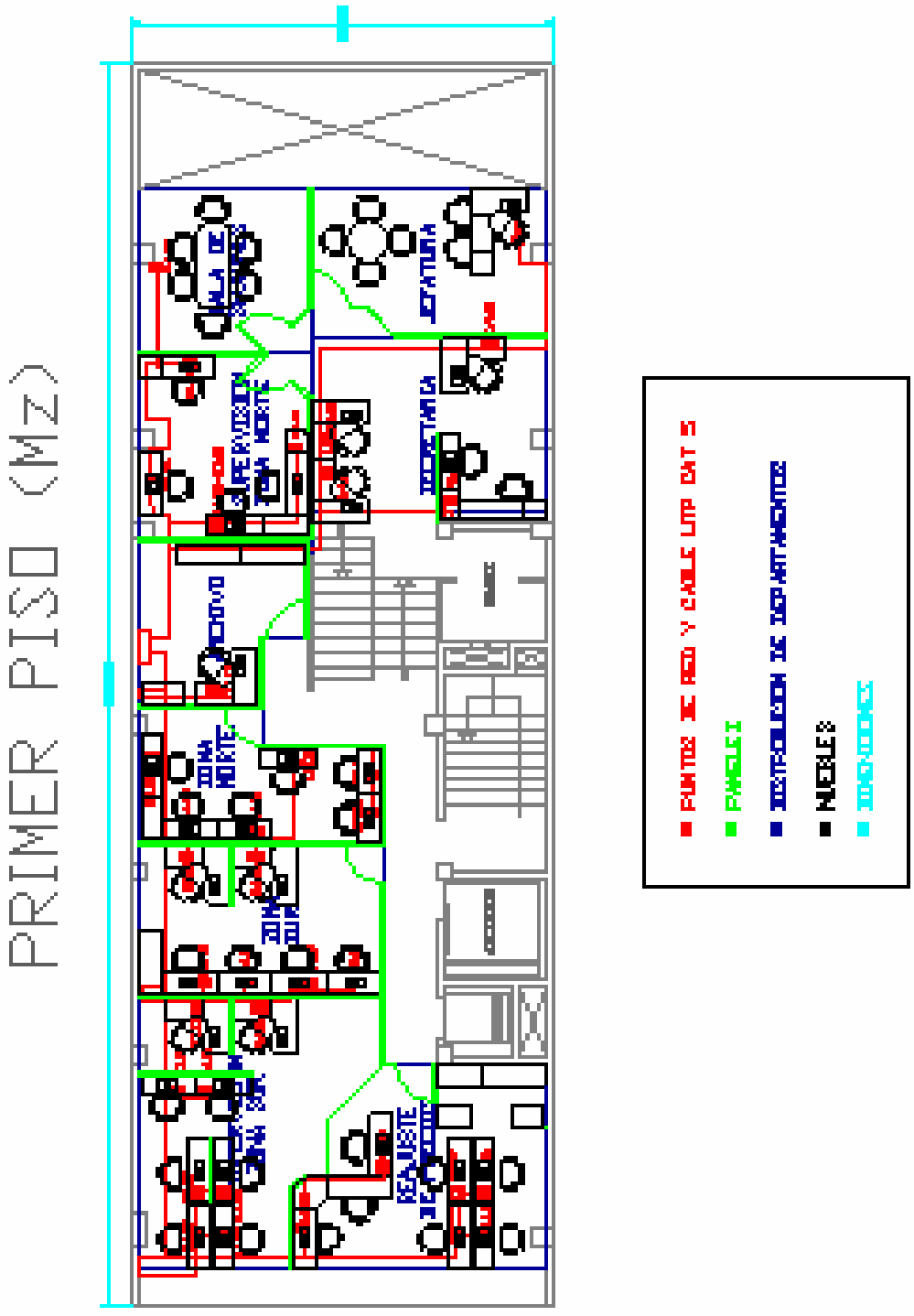


Figura 3.8. Primer Piso.

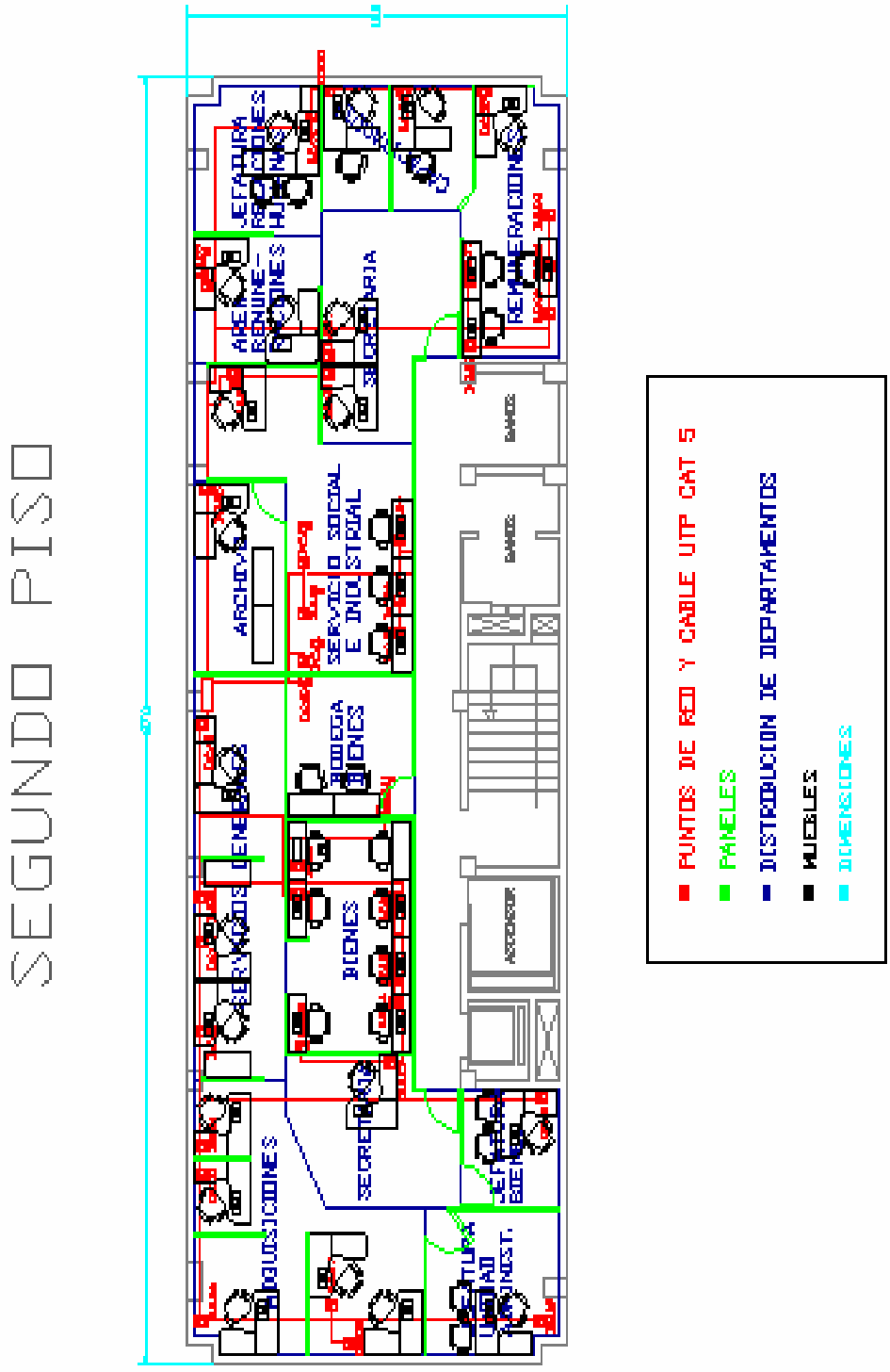


Figura 3.9. Segundo Piso.

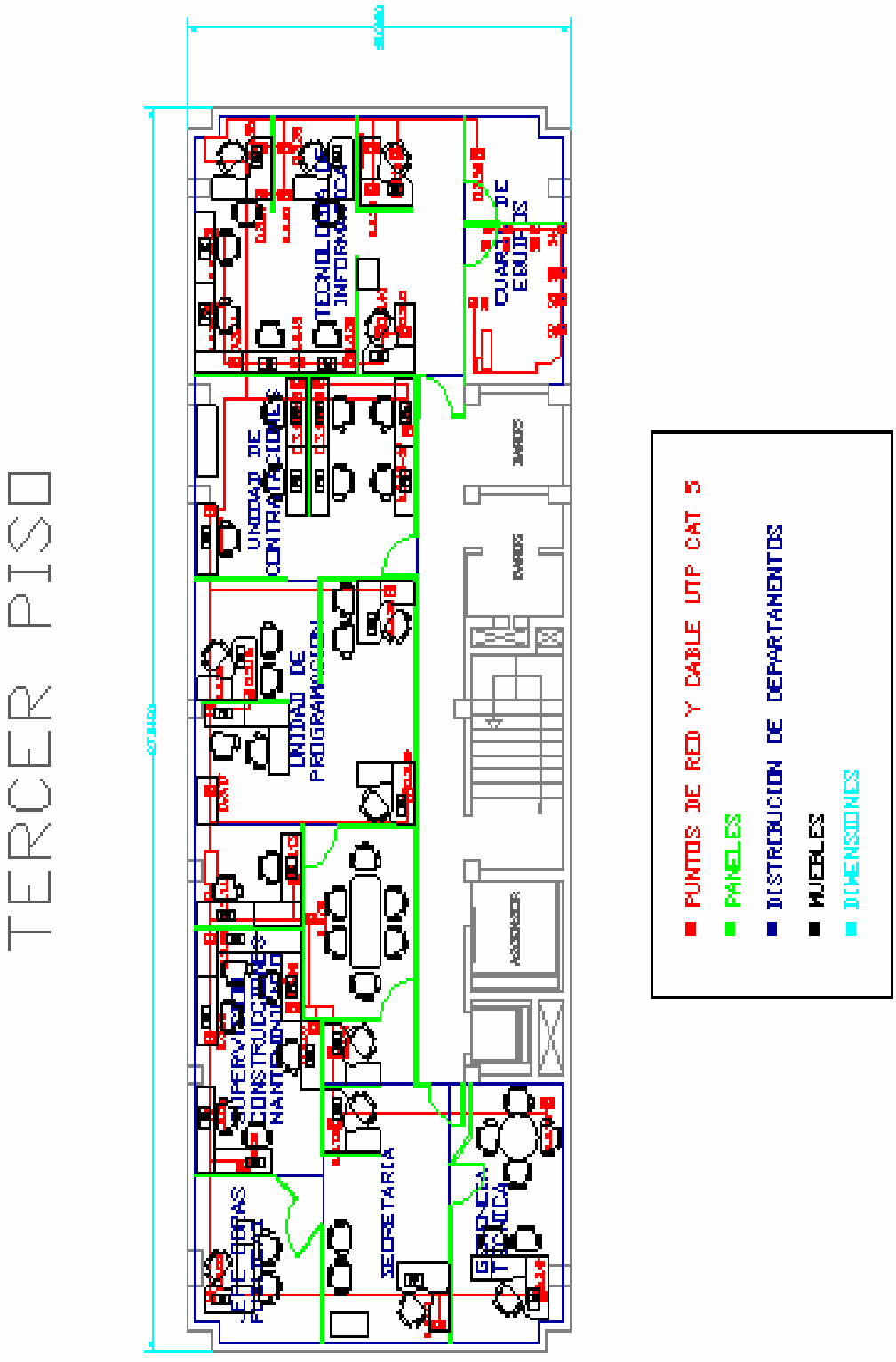


Figura 3.10. Tercer Piso.

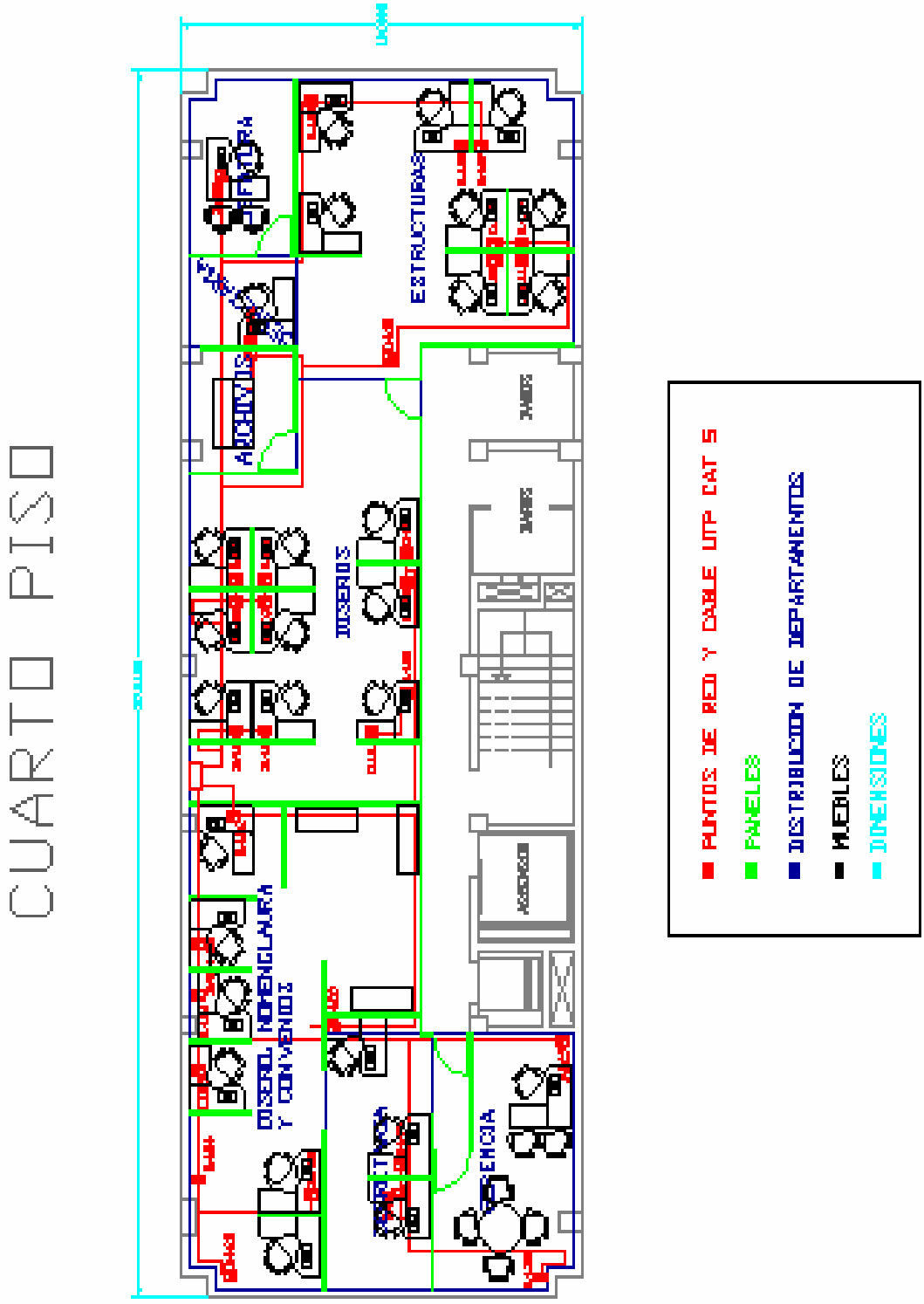


Figura 3.11. Cuarto Piso.

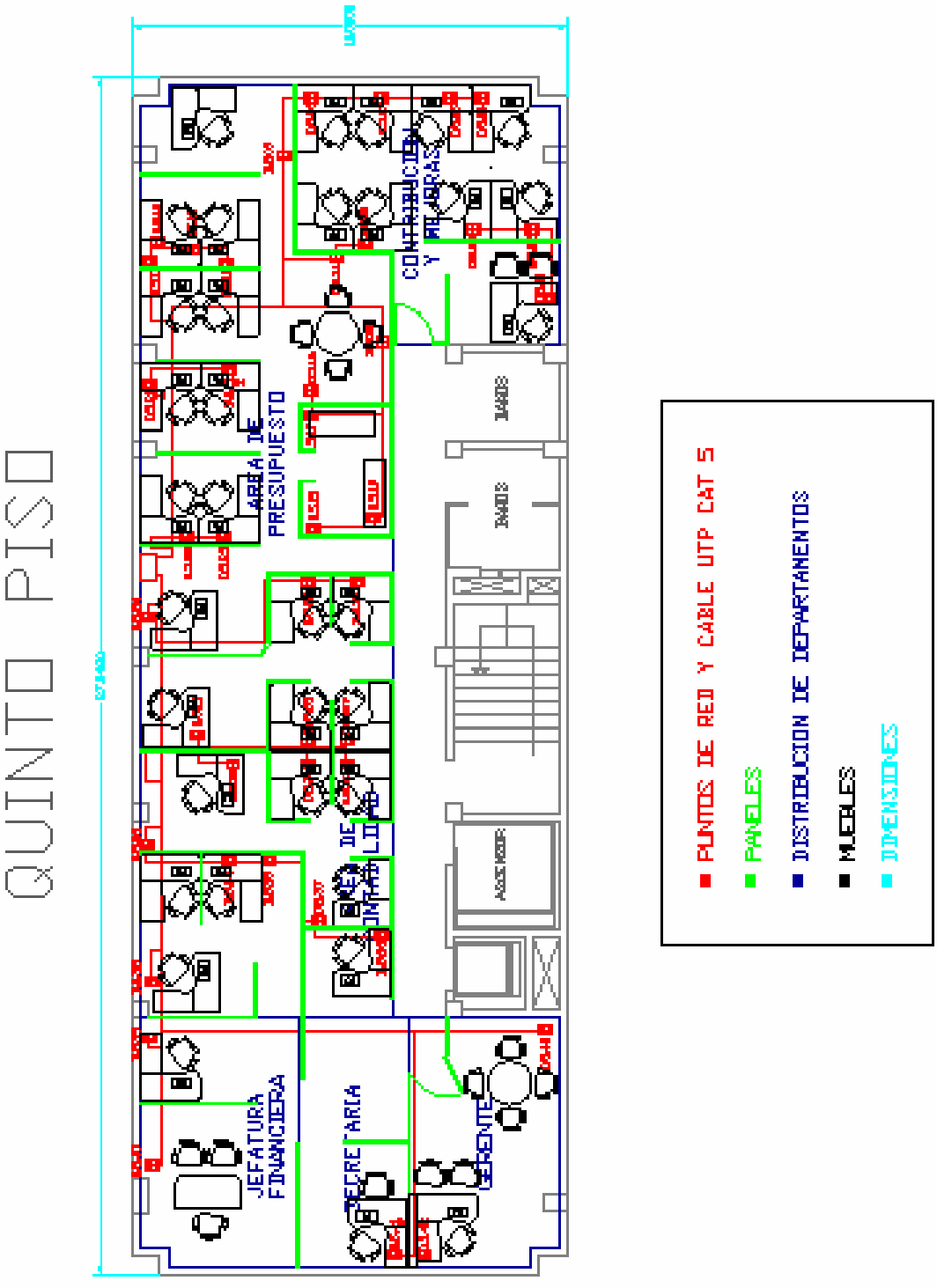


Figura 3.12. Quinto Piso.

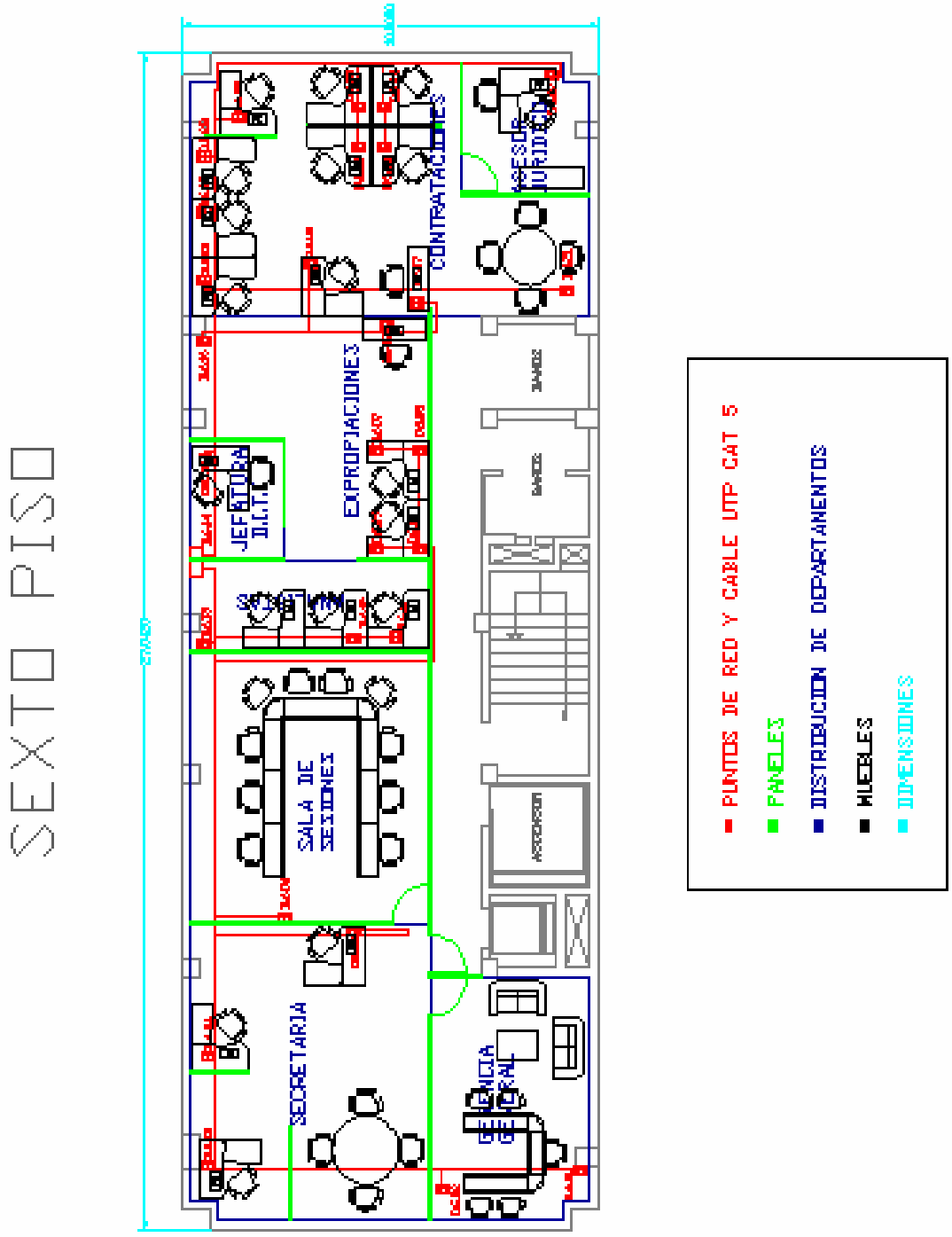


Figura 3.13. Sexto Piso.

3.5 SELECCIÓN DE EQUIPOS INALÁMBRICOS

Los equipos que se usan comúnmente para redes inalámbricas son los que utilizan el estándar IEEE 802.11g pero en la actualidad existen equipos inalámbricos que han sido desarrollados bajo nuevas tecnologías logrando así llegar a velocidades máximas de 108 Mbps. Esta tecnología está siendo implementada en productos con 802.11g.

3.5.1 Comparación entre marcas más destacadas.

Para realizar este estudio se han seleccionado tres marcas de equipos wireless para analizar sus características de funcionamiento como son: rendimiento, cobertura, compatibilidad, seguridad y disponibilidad y así elegir los equipos que más se adapten a las necesidades de la red. Las marcas elegidas son Belkin, Linksys-Cisco y D-Link ya que en estas marcas los equipos son de fácil adquisición en el mercado y tienen costos convenientes.

La siguiente tabla indica de manera general las principales características de los access points inalámbricos de las marcas mencionadas anteriormente.

	Belkin	**Linksys-Cisco**	**D-Link**
Modelo	F5D7130	WRT300N	DWL-7200AP
Descripción	Dualband Wireless G Access Point	Wireless-N Broadband Access Point	Dualband Wireless Access Point with PoE
Estándares	802.11b 802.11g	802.11b 802.11g	802.11b 802.11g

Opinión de usuarios(*)	(3.00/5.00)	(1.57/5.00)	(3.46/5.00)
Velocidad de transmisión	Hasta 54 Mbps	Hasta 108 Mbps	Hasta 108 Mbps
Tecnología De modulación	OFDM	OFDM	OFDM
Cobertura	Muy Buena	Buena	Muy Buena
Antenas	2	2	2
Configuración	Alta	Alta	Muy Alta
Administración	Media	Media	Alta
Seguridad Inalámbrica	PSK, WEP - 128-bit, WEP - 64-bit, WPA	WEP - 128-bit, WEP - 256-bit, WEP - 64-bit, WPA,	PSK, WEP - 128-bit, WEP - 64-bit, WPA,
Precio Aproximado	$ 120	$ 154	$ 175

(*) Referencia www.ecoustics.com

Tabla 3.2. Tabla comparativa de equipos inalámbricos.

3.5.2 Selección de equipos

Después de haber realizado un análisis previo con cada uno de los equipos indicados se ha seleccionado a D-Link como la mejor opción en equipos para el diseño y la implementación de la red inalámbrica por cuatro razones esenciales que son:

- Alto nivel de cobertura, configuración y administración.
- Seguridad inalámbrica confiable.
- Costos accesibles.
- Configuración amigable.

El hecho de que se obtenga buena cobertura y administración confiable hace que la red inalámbrica tenga un nivel de funcionamiento mejorado ya que se puede realizar configuraciones avanzadas que los otros equipos no ofrecen.

3.6 ACCESS POINT DWL-7200AP

3.6.1 Revision de Hardware

El access point DWL-7200AP tiene las siguientes medidas:

- Largo: 17.5 cm.
- Ancho: 10.5 cm.
- Altura: 2 cm.
- Peso: 200 g.

Panel Frontal

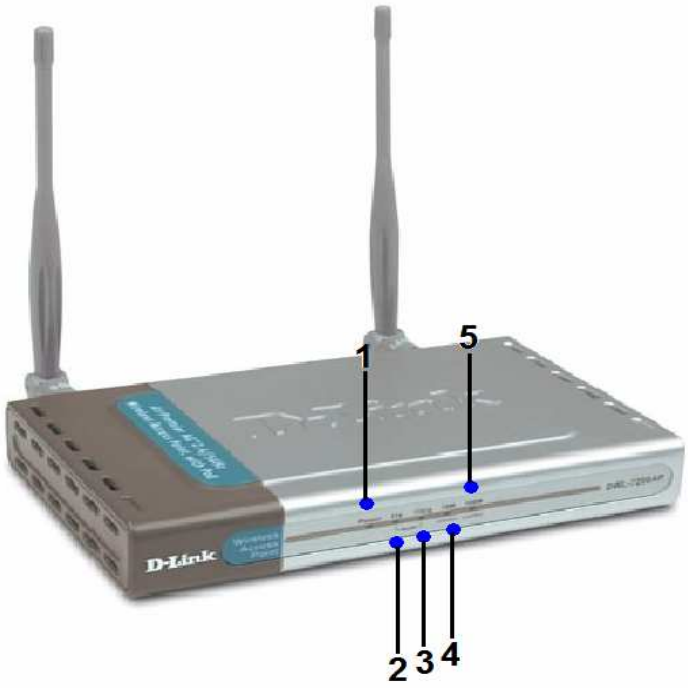


Figura 3.14. Panel frontal del access point D-Link DWL-7200AP.

1. Power Led: La luz verde sólida indica una apropiada conexión con la fuente de poder.

2. **11 a led:** La luz verde sólida indica actividad WLAN 802.11a. Este led destella durante la transmisión de datos.
3. **11 b/g Led:** La luz verde sólida indica actividad WLAN 802.11b y g. Este led destella durante la transmisión de datos.
4. **10M led:** La luz verde destellante indica actividad en el puerto ethernet con velocidad de transferencia de datos de hasta 10 Mbps.
5. **100M Led:** La luz verde destellante indica actividad en el puerto fast ethernet con velocidad de transferencia de datos de hasta 100 Mbps.

Panel Posterior

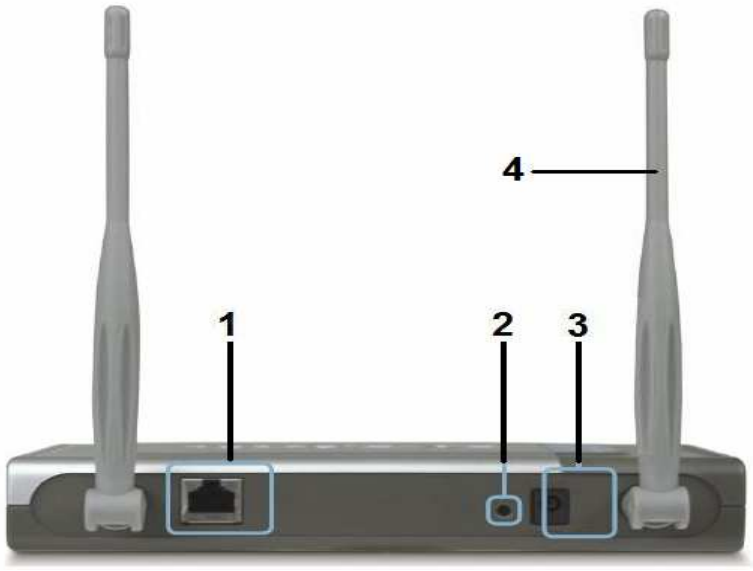


Figura 3.15. Panel posterior access point D-Link DWL-7200AP.

1. **Puerto LAN:** Puertos MDI/MDIX. Estos puertos censan automática-mente el tipo de cable cuando es conectado a la red local.
2. **Botón de reset:** El botón reset regresa a la configuraron original de fábrica. Al presionar y soltar el botón el access point se reseteará en 10 segundos.

3. **Conector DC:** Conector de poder DC al que se conecta una fuente de poder de 5V 3A.
4. **Antenas:** Dos antenas externas con una ganancia de 5dBi.

3.6.2 Características

- Completamente compatible con el estándar 802.11g para proveer una taza de datos inalámbricos de hasta 108 Mbps.
- WPA (Wi-Fi Protected Access) autoriza e identifica a usuarios basados en una combinación secreta que cambia automáticamente en un intervalo de tiempo regular.
- Utiliza tecnología OFDM.
- Consta de un utilitario amigable de configuración y diagnostico que facilita la instalación y la administración del equipo.
- Opera en la banda de 2.4 GHz y 5GHz. Tiene la capacidad de operar en las dos bandas al mismo tiempo.
- Filtrado de direcciones MAC. Para seguridad adicional, se puede establecer una lista de direcciones MAC (identificadores de cliente únicos) que tengan permiso de acceso a la red.
- Filtrado de direcciones IP. Se puede realizar un lista de direcciones IP que tengan permiso para conectarse a la red. Esto requiere que la tarjeta de red sea configurada con una dirección IP específica para que pueda ser reconocida.
- Servidor DHCP (Dinamic Host Control Protocol), protocolo de configuración de host dinámico integrado hace que sea la conexión más sencilla de una red. El servidor DHCP le asignará direcciones IP a cada computador automáticamente para que no necesite hacer instalaciones complicadas de la red.
- Configuración y administración por interfase Web. El equipo es totalmente configurable por medio de un Browser (explorador de Internet).
- 5 modos diferentes de operación, el access point es capaz de funcionar también como repetidor, puente punto a punto, puente punto a multipunto y como cliente inalámbrico.

3.7 MAPAS DE COBERTURA

Los mapas de cobertura son gráficos que indican la expansión de la señal de los equipos inalámbricos basándose en las características de las antenas. Este equipo tiene antenas omnidireccionales de 5dBi de ganancia las cuales cubren 360^{o} en forma horizontal y 30^{o} en forma vertical.

Para las mediciones de nivel de señal se utilizó el Cliente Intel PROSet Wireless que se incluye con el adaptador de red inalámbrica Intel® PROSet/Wireless 2200BG Network Connection. Este cliente ofrece visión del nivel de señal dividido en cinco barras como se indicara más adelante, también muestra el estado de la tarjeta inalámbrica (conectado, no conectado), la potencia de transmisión en dBm (RSSI) y el nombre de la red inalámbrica a la que está conectado.

Para las pruebas de estado de conexión se utiliza el comando “PING” que se trata de una utilidad que comprueba el estado de la conexión con uno o varios equipos remotos, por medio de los paquetes de solicitud de eco y de respuesta de eco (definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP. También se utiliza para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos, este tiempo es el que va a tomar en cuenta en las mediciones a realizar.

3.7.1 Cobertura Horizontal

Se realizaron mediciones a distancias de 3 metros desde el centro de cada piso donde se ubicó el access point y se tabularon los siguientes datos haciendo un promedio de varias pruebas, a las mismas distancias, de todos los pisos. Se enviaron entre 40 y 50 paquetes de datos y se toma un promedio del tiempo en el que se recibe la respuesta de los paquetes enviados. En los siguientes gráficos se presentan de las mediciones más críticas realizadas obteniendo una información promedio de todos los pisos.

A 3 metros del equipo inalámbrico:

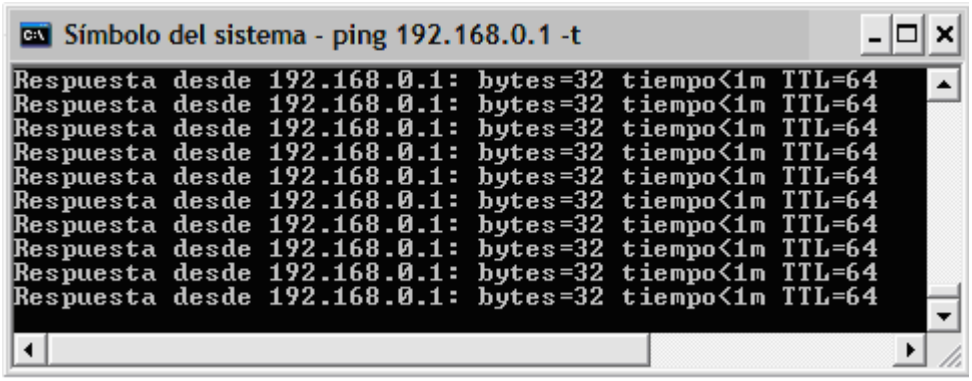


Figura 3.16. Comando ping a 3 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 0ms. Máximo: 0ms. Promedio: 0ms.

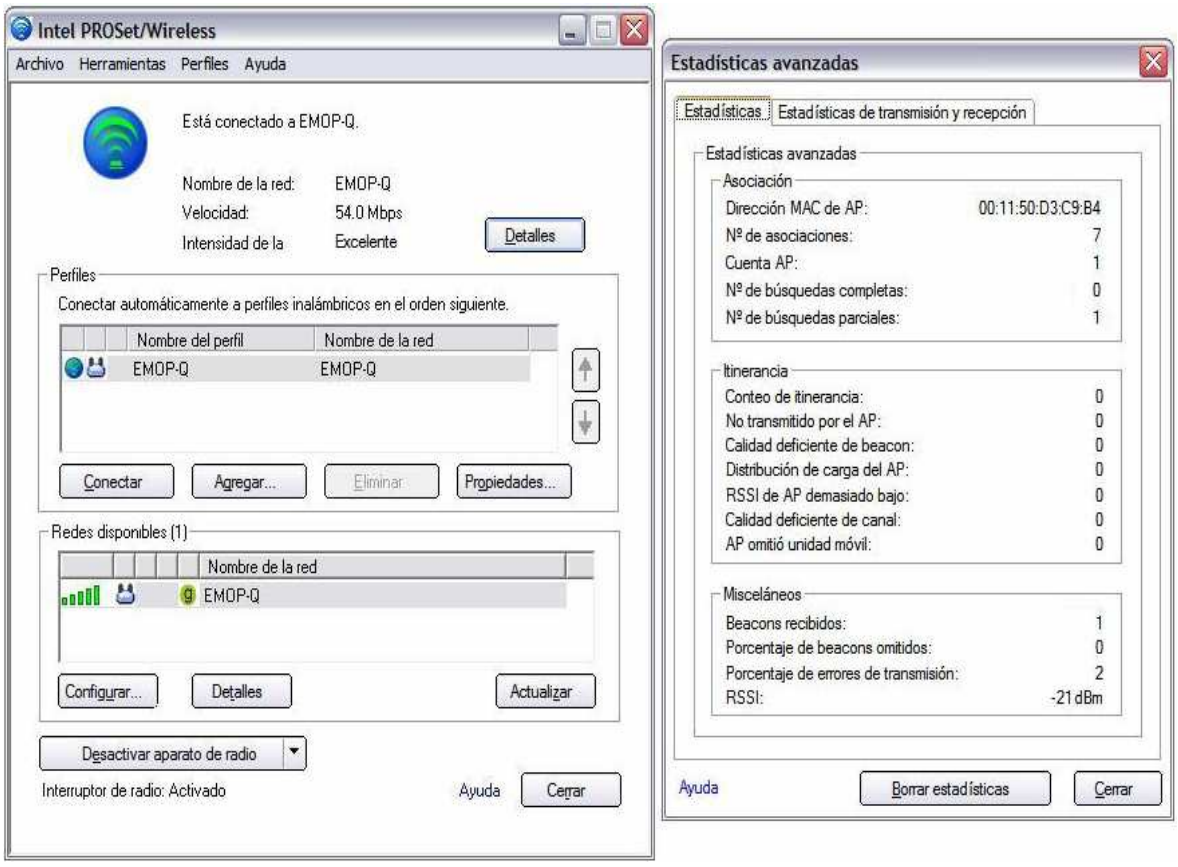


Figura 3.17. Nivel de señal y velocidad de conexión a 3 metros.

A 6 metros del equipo inalámbrico:

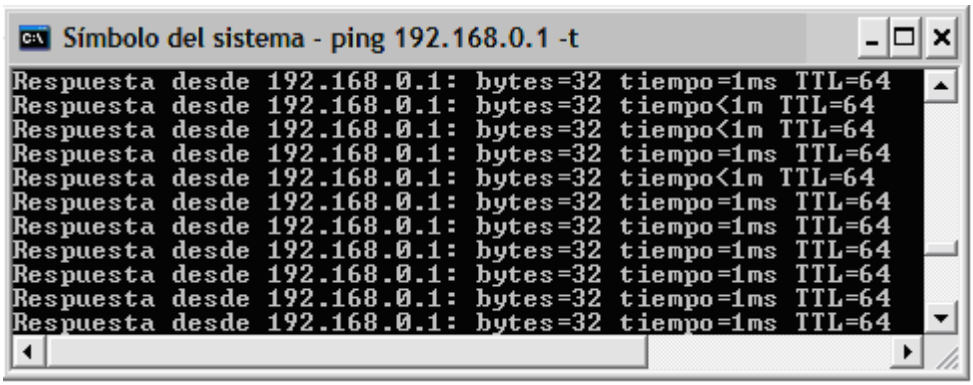


Figura 3.18. Comando ping a 6 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 0ms. Máximo: 1ms. Promedio: 1ms.

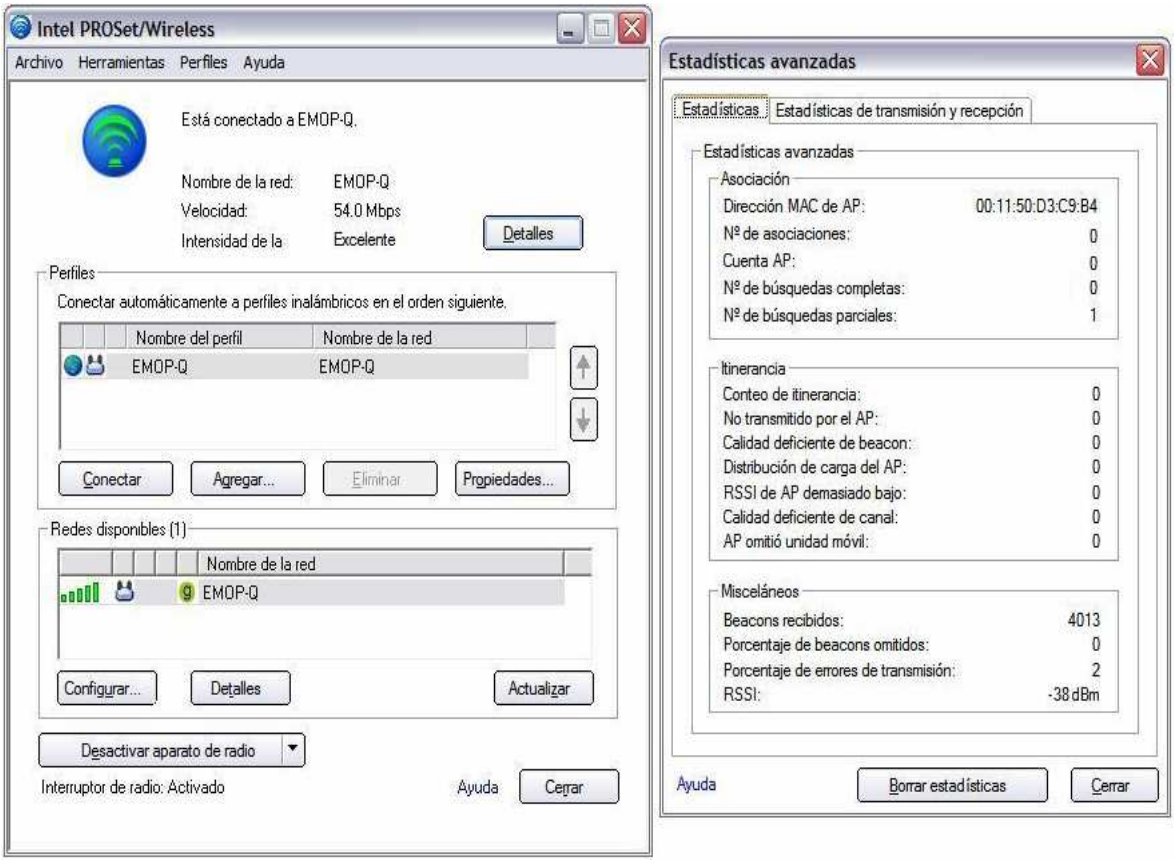


Figura 3.19. Nivel de señal y velocidad de conexión a 6 metros.

A 9 metros del equipo inalámbrico:

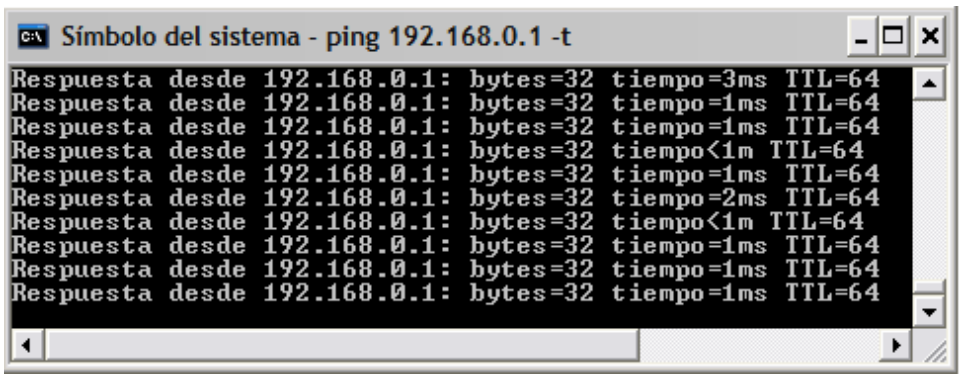


Figura 3.20. Comando ping a 9 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: <1ms. Máximo: 3ms. Promedio: 1ms.

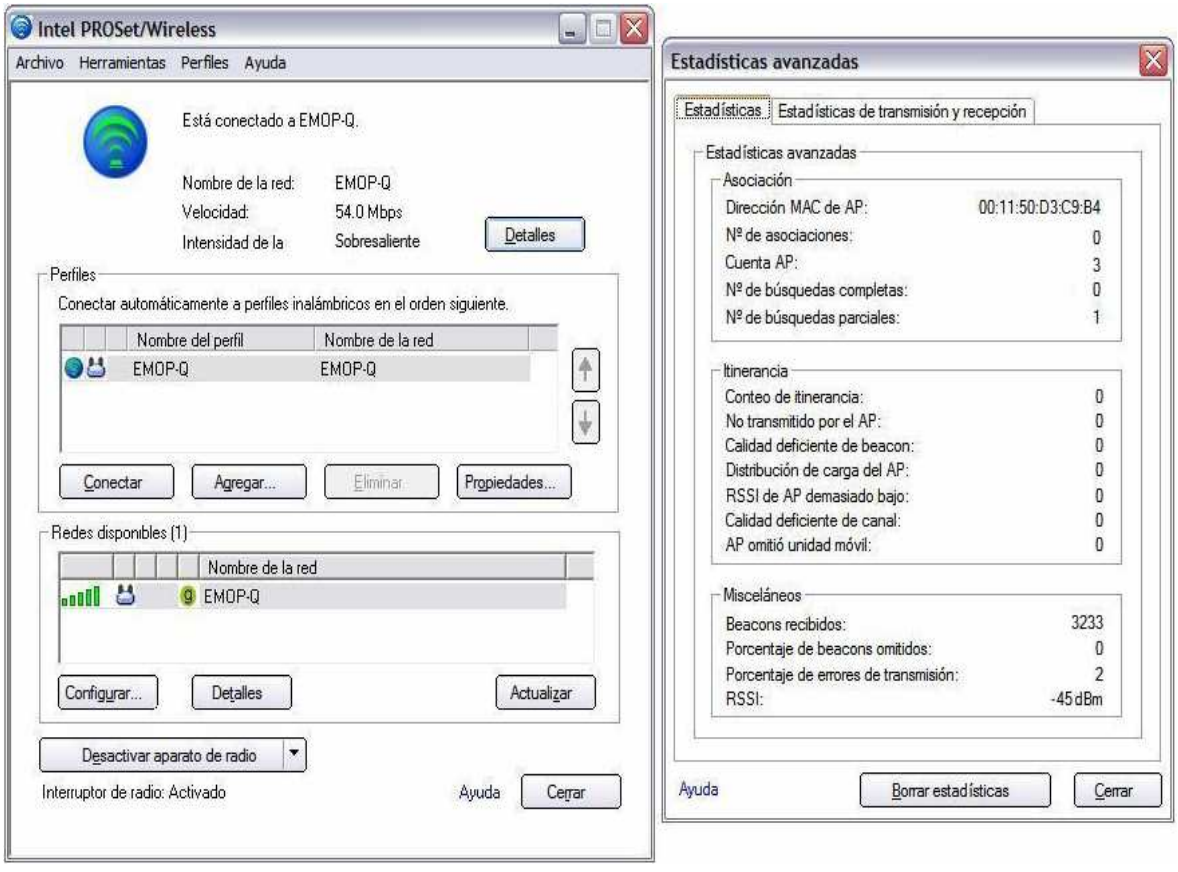


Figura 3.21. Nivel de señal y velocidad de conexión a 9 metros.

A 12 metros del equipo inalámbrico:

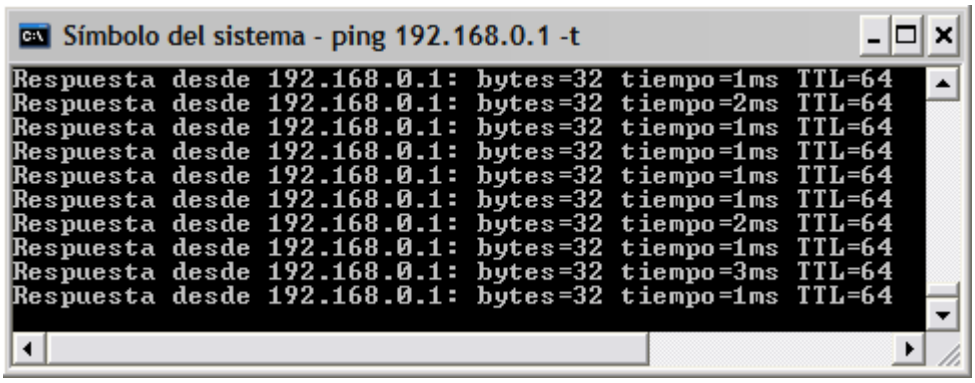


Figura 3.22. Comando ping a 12 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 1ms. Máximo: 3ms. Promedio: <2ms.

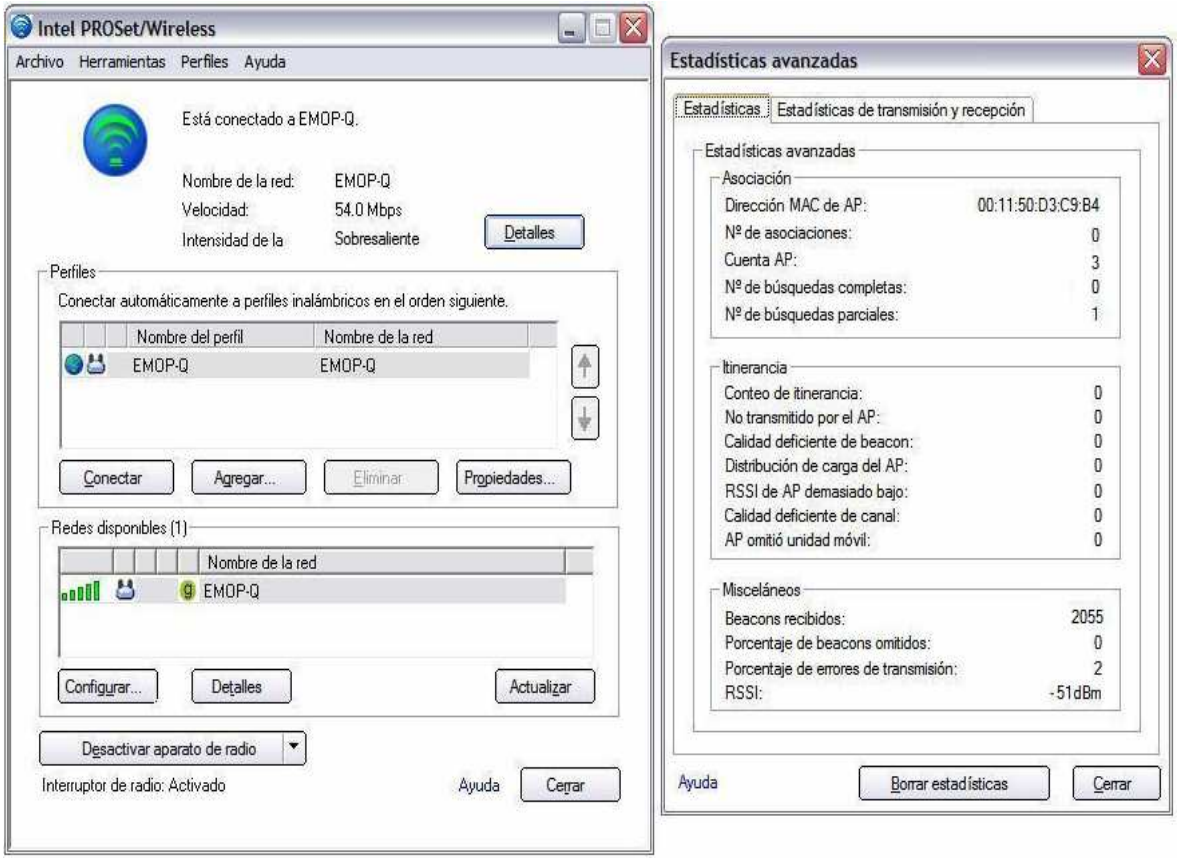


Figura 3.23. Nivel de señal y velocidad de conexión a 12 metros

A ~15 metros del equipo inalámbrico:

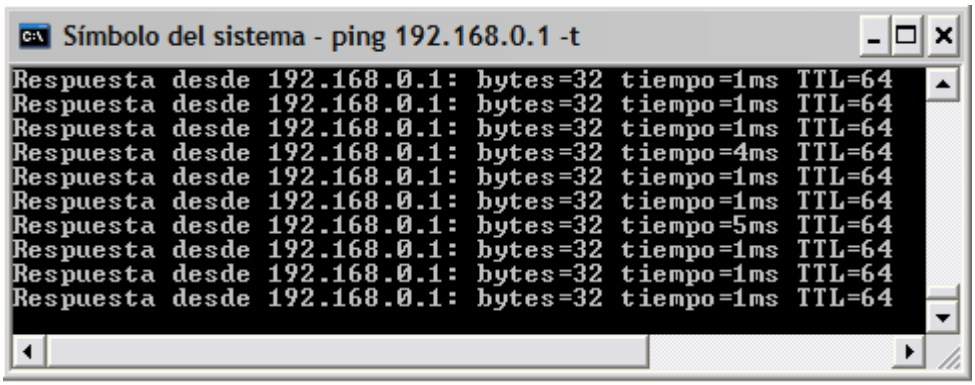


Figura 3.24. Comando ping a ~15 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 1ms. Máximo: 5ms. Promedio: <2ms.

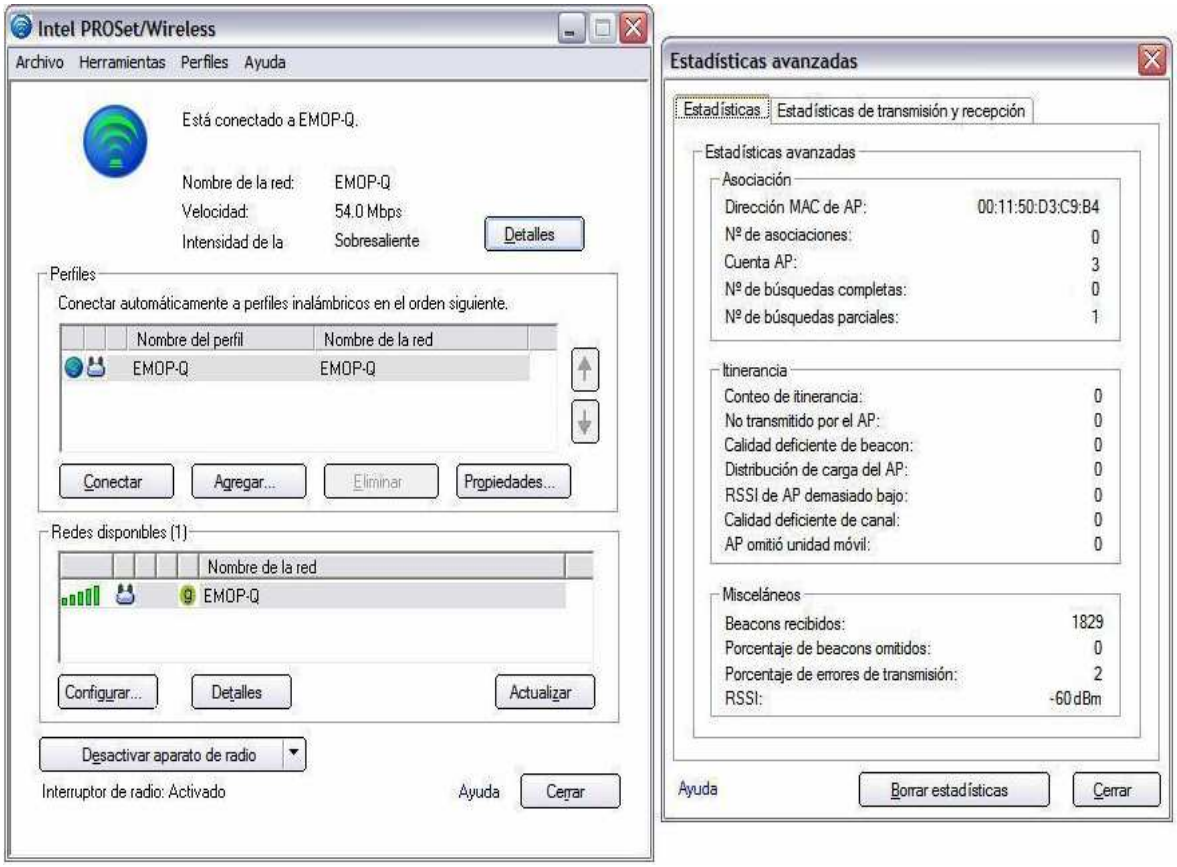
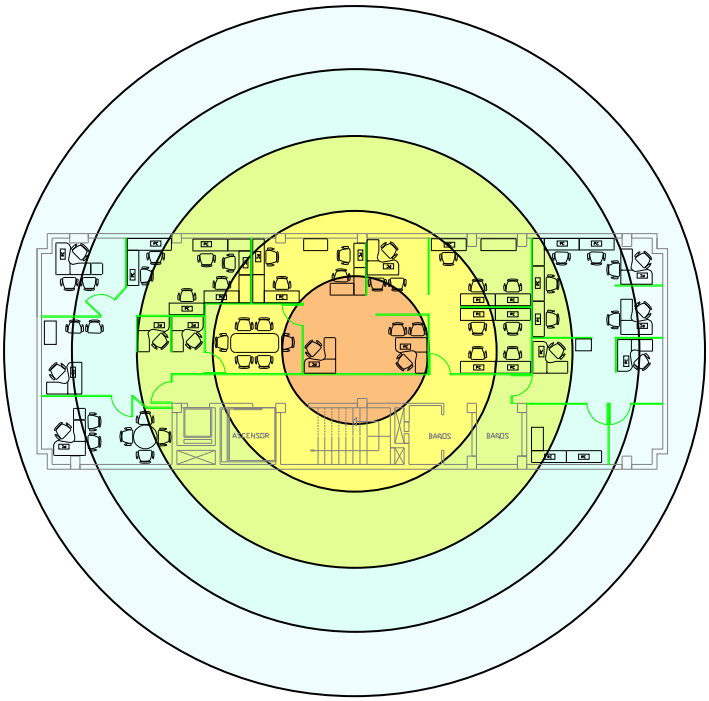


Figura 3.25. Nivel de señal y velocidad de conexión a ~15 metros.

Se puede notar que a medida que se aleja un host del equipo inalámbrico la señal va perdiendo fuerza y el tiempo de respuesta de un “ping” es mayor pero la variación es muy pequeña y se obtiene un buen nivel de señal y velocidad de conexión en el punto mas lejano (aproximadamente 13 metros) debido a las características indicadas anteriormente.

Con esto, se puede tener una idea gráfica de los niveles de señal y las velocidades de conexión resumidas en el siguiente esquema.



DISTANCIA	0 a 3 m.	3 a 6 m.	6 a 9 m.	9 a 12 m.	12 a ~15 m.
VELOCIDAD	54 Mbps.	54 Mbps.	54 Mbps.	54 Mbps.	54 Mbps.
POTENCIA	-9; - 21 dBm	-22; - 38 dBm	-39; - 45 dBm	-46; - 51 dBm	-52; - 60 dBm

Figura 3.26. Esquema de Cobertura horizontal

3.7.2 Cobertura vertical:

El análisis de cobertura vertical se ha realizado en forma similar a la horizontal, en este caso se realizan mediciones en los pisos superior e inferior en relación al piso en el que se encuentra el access point. Los resultados son los siguientes.

A 3 metros del equipo inalámbrico:

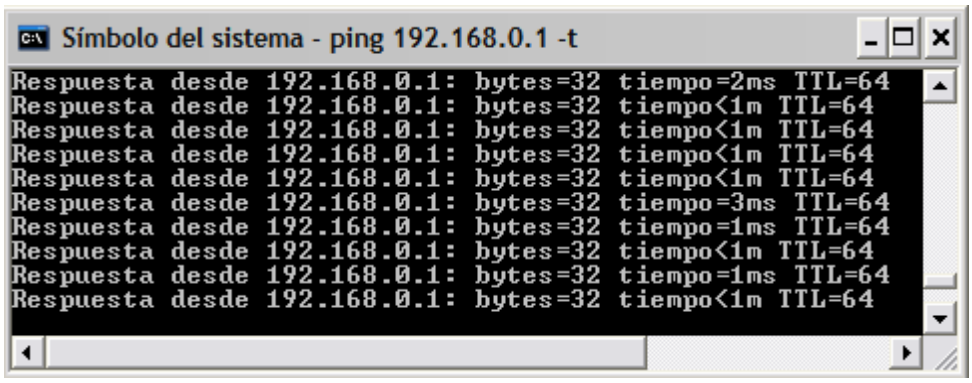


Figura 3.27. Comando ping a 3 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 0ms. Máximo: 3ms. Promedio: 1ms.

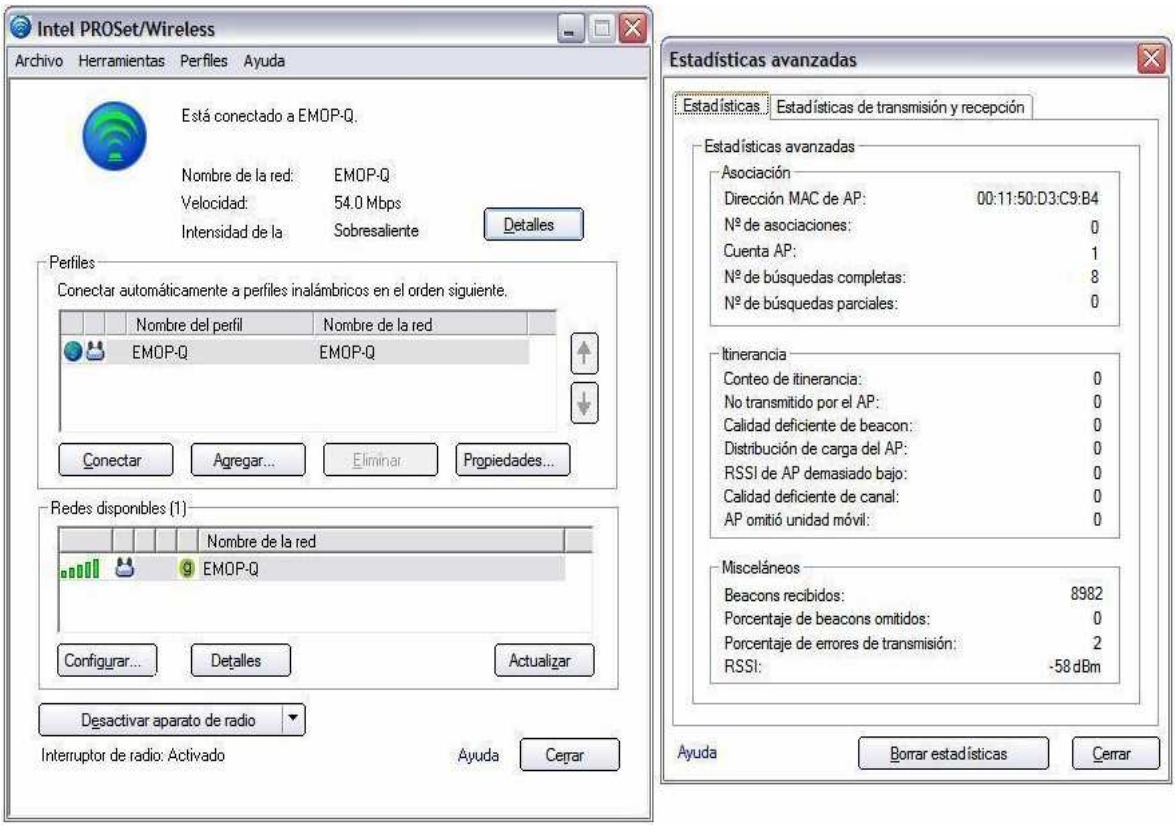


Figura 3.28. Nivel de señal y velocidad de conexión a 3 metros.

A 6 metros del equipo inalámbrico:

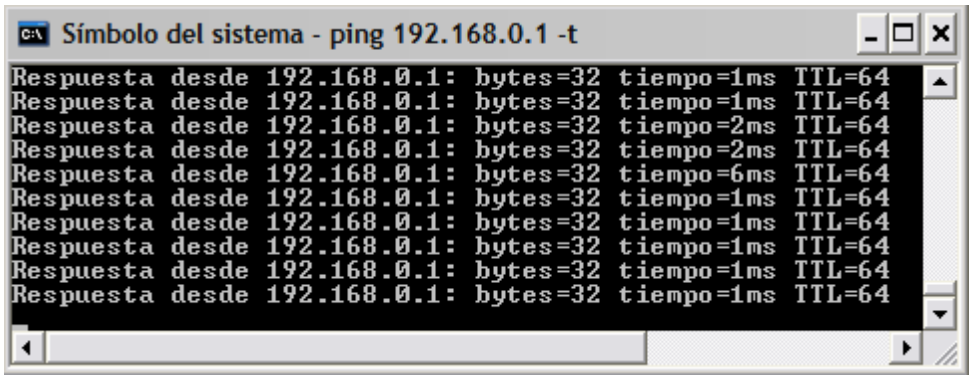


Figura 3.29. Comando ping a 6 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 1ms. Máximo: 6ms. Promedio: 2ms.

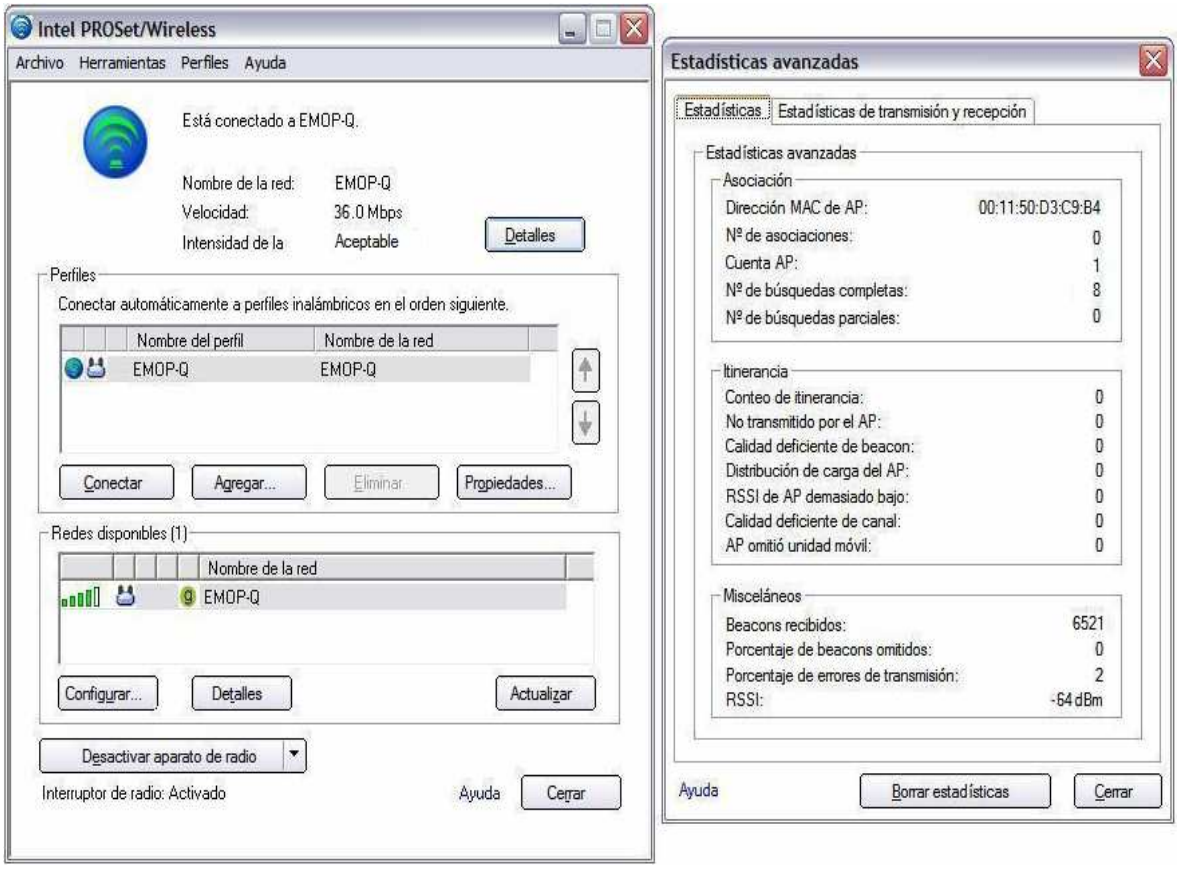


Figura 3.30. Nivel de señal y velocidad de conexión a 6 metros.

A 9 metros del equipo inalámbrico:

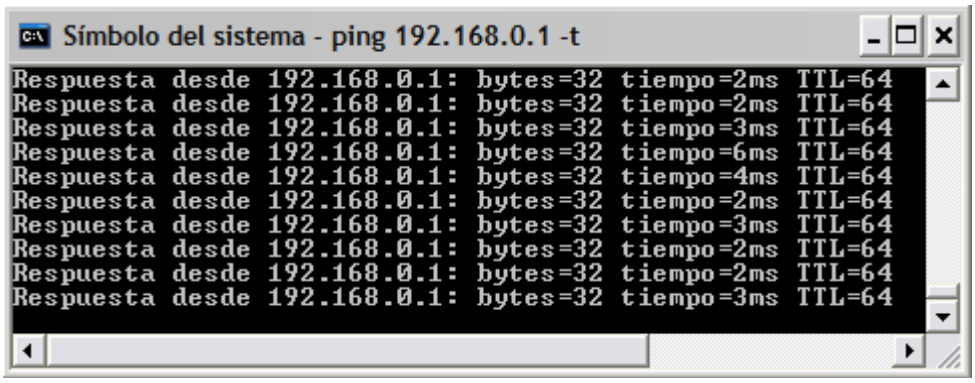


Figura 3.31. Comando ping a 9 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 2ms. Máximo: 6ms. Promedio: 3ms.

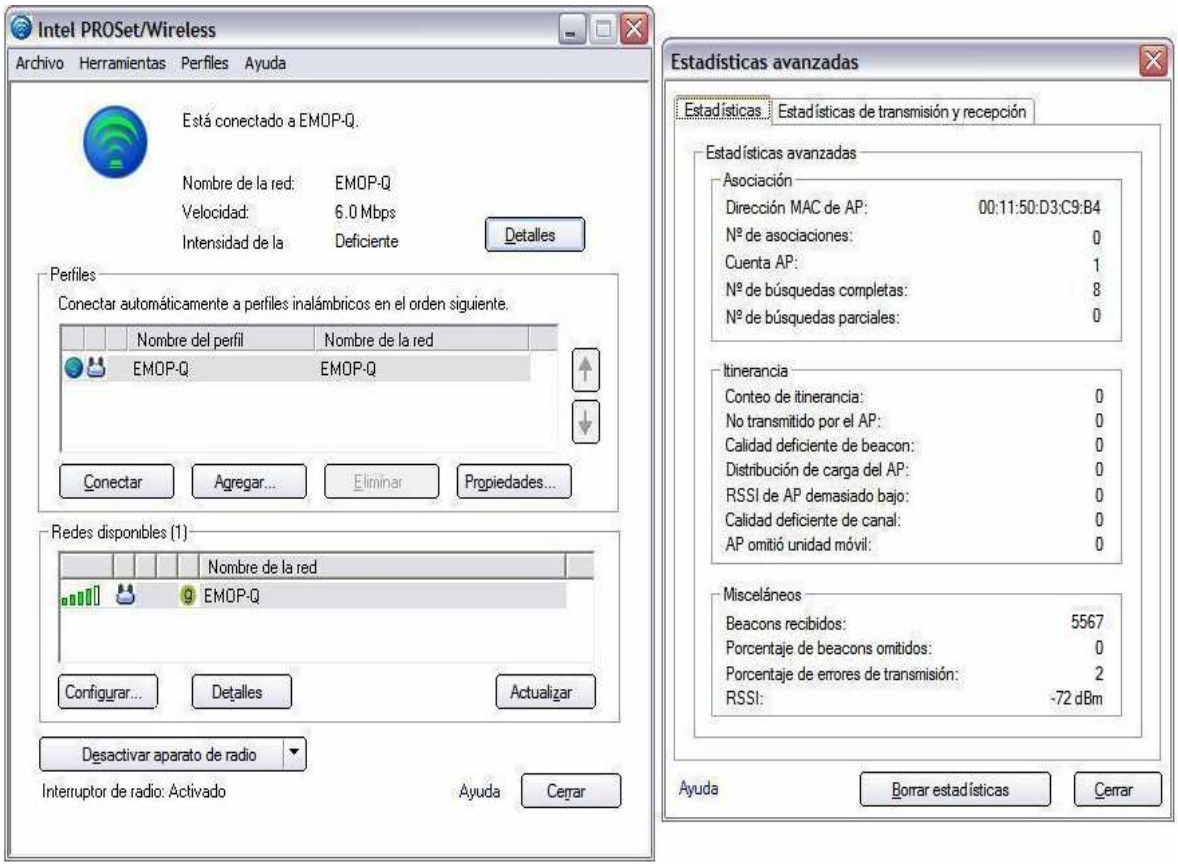


Figura 3.32. Nivel de señal y velocidad de conexión a 9 metros.

A 12 metros del equipo inalámbrico:

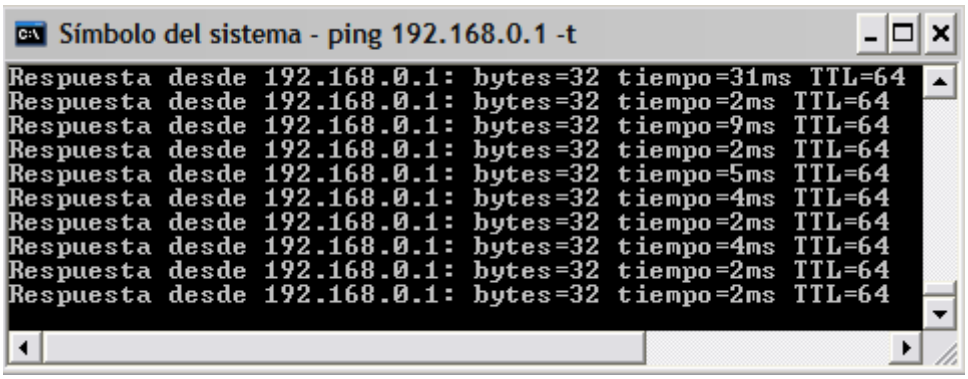


Figura 3.33. Comando ping a 12 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 2ms. Máximo: 31ms. Promedio: 6ms.

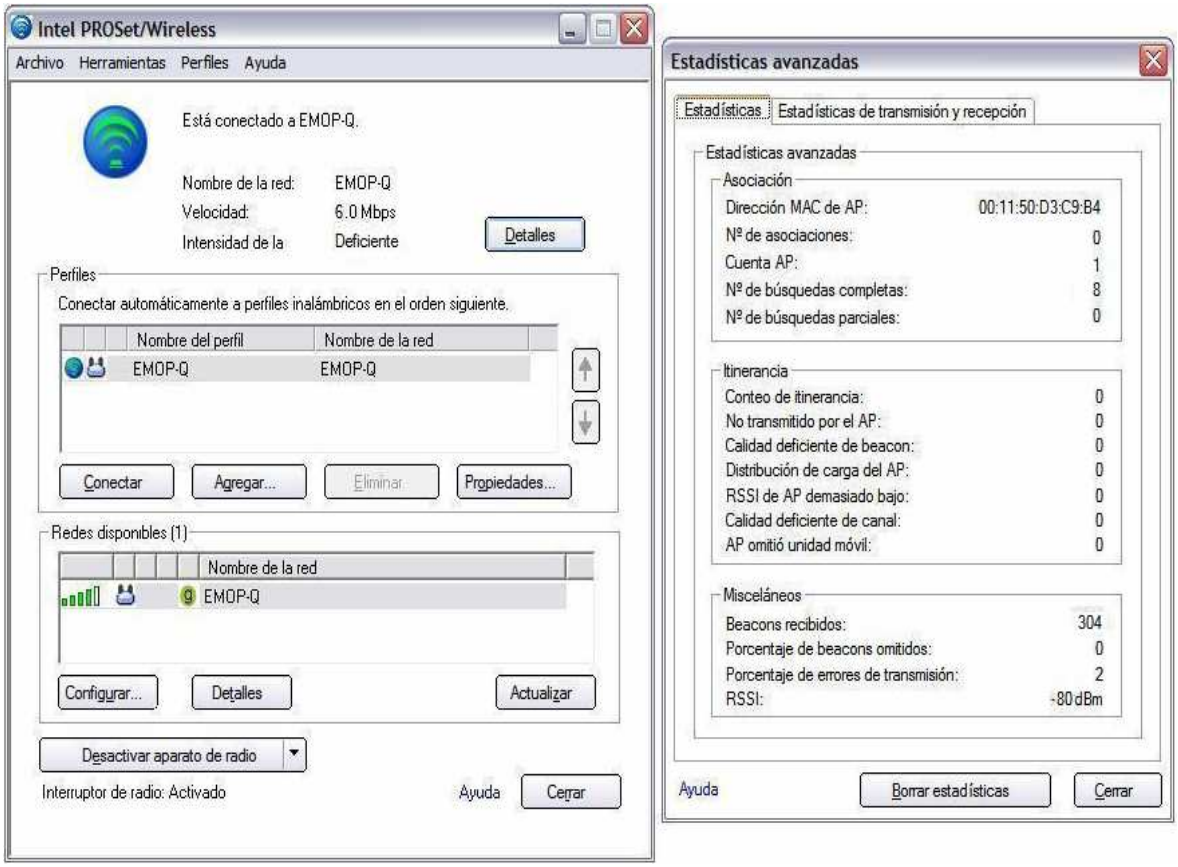


Figura 3.34. Nivel de señal y velocidad de conexión a ~15 metros.

A ~15 metros del equipo inalámbrico:

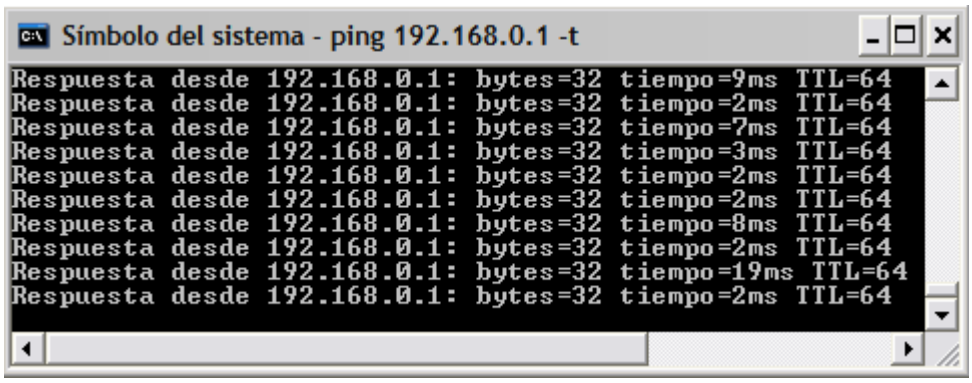


Figura 3.35. Comando ping a ~15 metros.

Paquetes enviados: 50 Paquetes recibidos: 50 Paquetes perdidos: 0

Tiempos aproximados de ida y vuelta:

Mínimo: 2ms. Máximo: 19ms. Promedio: 6ms.

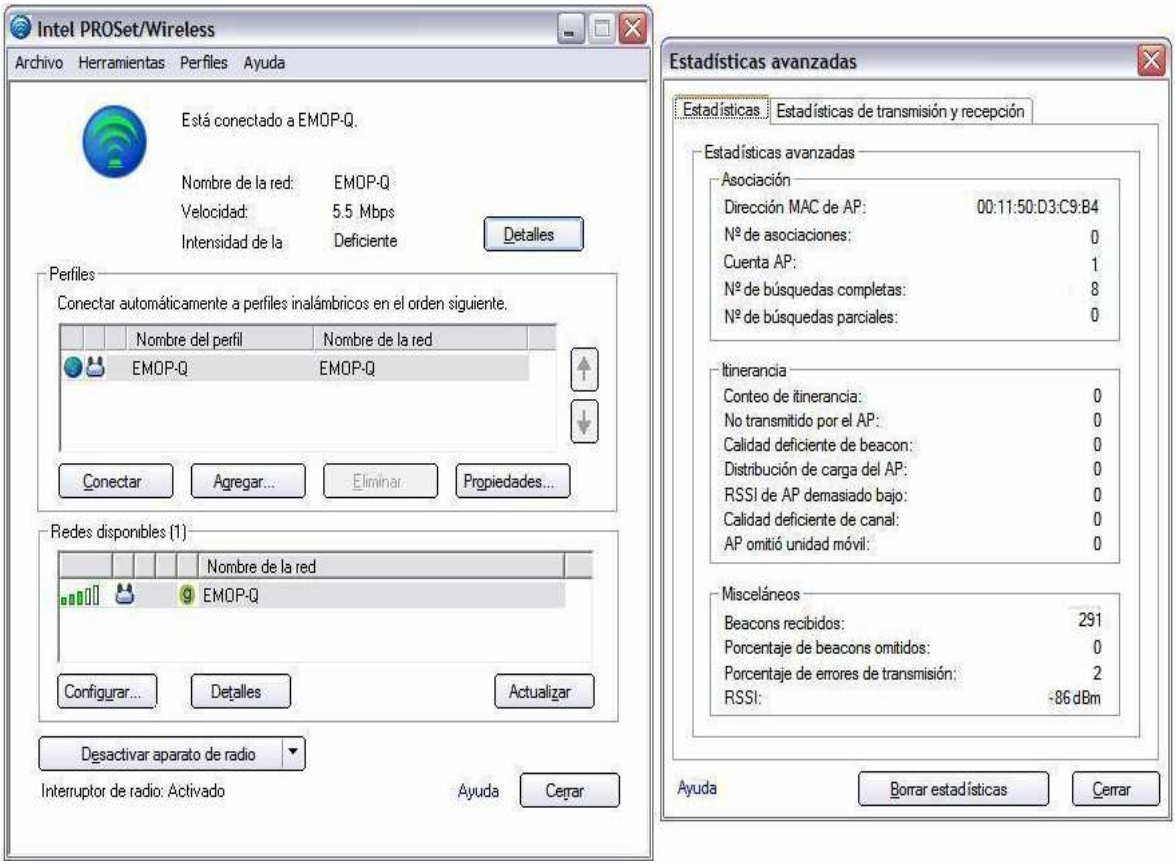
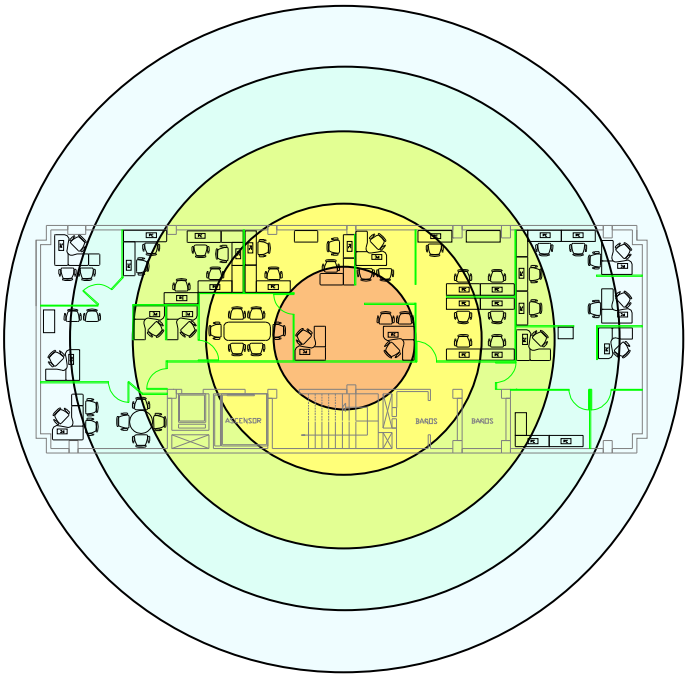


Figura 3.36. Nivel de señal y velocidad de conexión a ~15 metros.

A continuación de presenta un gráfico resumen con las mediciones promedio realizadas en los pisos superior e inferior con relación al piso donde se encuentra el access point.



DISTANCIA	0 a 3 m.	3 a 6 m.	6 a 9 m.	9 a 12 m.	12 a ~15 m.
VELOCIDAD	54 Mbps.	36 Mbps.	6 Mbps.	6 Mbps.	5.5 Mbps.
POTENCIA	-52; - 58 dBm	-59; - 64 dBm	-65; - 72 dBm	-73 - 80 dBm	-81; - 86 dBm

Figura 3.37. Esquema de Cobertura vertical

Podemos ver que la potencia de transmisión es muy baja entre un piso y otro como para cubrir toda esa área con un solo equipo. De igual forma que en la cobertura horizontal, la señal se va debilitando mientras la distancia aumenta pero en este caso la señal se debilita mucho mas ya que intenta cruzar el techo que es de un material muy atenuante como el hierro y el cemento.

En el siguiente gráfico se muestran los valores de sensibilidad de recepción del equipo para verificar que los valores que se obtuvieron en las mediciones están dentro de los parámetros normales de funcionamiento del equipo y por lo que no se obtiene ningún inconveniente con este diseño.

Receiver Sensitivity

For 802.11a:

- 6Mbps: -87dBm
- 9Mbps: -86dBm
- 11Mbps: -88dBm
- 12Mbps: -85dBm
- 18Mbps: -83dBm
- 24Mbps: -80dBm
- 36Mbps: -76dBm
- 48Mbps: -71dBm
- 54Mbps: -71dBm

For 802.11b:

- 1Mbps: -92dBm
- 2Mbps: -89dBm
- 5.5Mbps: -88dBm
- 11Mbps: -83dBm

For 802.11g:

- 1Mbps: -95dBm
- 2Mbps: -91dBm
- 5.5Mbps: -89dBm
- 6Mbps: -87dBm
- 9Mbps: -85dBm
- 11Mbps: -88dBm
- 12Mbps: -80dBm
- 18Mbps: -80dBm
- 24Mbps: -77dBm
- 36Mbps: -73dBm
- 48Mbps: -72dBm
- 54Mbps: -72dBm

Figura 3.38. Sensibilidad del equipo

Al analizar los resultados de las diferentes pruebas se llega a determinar que es necesario ubicar un access point por piso para tener una buena cobertura ya que, por los valores obtenidos en la cobertura vertical, la señal no pasa de un piso a otro con la potencia necesaria para tener una conexión de alta velocidad.

Con un equipo en cada piso se logra cubrir toda el área de trabajo con un buen nivel de señal y con un tiempo de envío y recepción de paquetes dentro de los rangos normales para una conexión inalámbrica.

3.8 DIRECCIONES IP PARA LA RED WLAN

Como sabemos que la red de la EMOP-Q tiene alrededor de 210 host habilitados y que su proyección de incremento a futuro es mínima, se ha considerado un incremento del 10 al 15% (de 20 a 35 host) de los host actuales dándonos un total de unos 235 host que se utilizarán en promedio en toda la red. A esta cantidad de direcciones se debe aumentar 7 que serán las que se asignen a los access points.

Para realizar la asignación de las direcciones en la red se ha seleccionado direcciones IP de clase C. Las redes de clase C van desde 192.0.0.0 hasta 223.255.255.0, con el número de red contenido en los tres primeros octetos y de

host en el último octeto. Esta clase permite cerca de 2 millones de redes con hasta 254 host´s.

Las redes privadas de organizaciones que no están directamente conectadas a Internet, es decir las redes que se conectan por medio de un proxy o un router a una única línea con una sola dirección IP dada por un proveedor de servicios, tienen asignado unos rangos de direcciones IP para su funcionamiento interno. Estos son:

- Para clase A una única dirección de red: 10
- Para clase B 16 redes del rango 172.16 a 172.31
- Para clase C 256 direcciones de red: 192.168.0 a 192.168.255

Estas direcciones IP no son utilizadas por los routers para su comunicación con Internet, y se utilizan solo dentro de la organización. Estas redes (Intranet) tienen la ventaja de ser mucho menos accesibles a ataques desde el exterior.

La dirección de red que asignamos es la 192.168.0.0 con mascara de subred 255.255.255.0 obteniendo así 254 direcciones IP habilitadas. Estas direcciones son ingresadas en el servidor DHCP para generar de forma dinámica todas las direcciones. La siguiente figura ilustra los octetos de las direcciones clase C privadas y la mascara de subred.

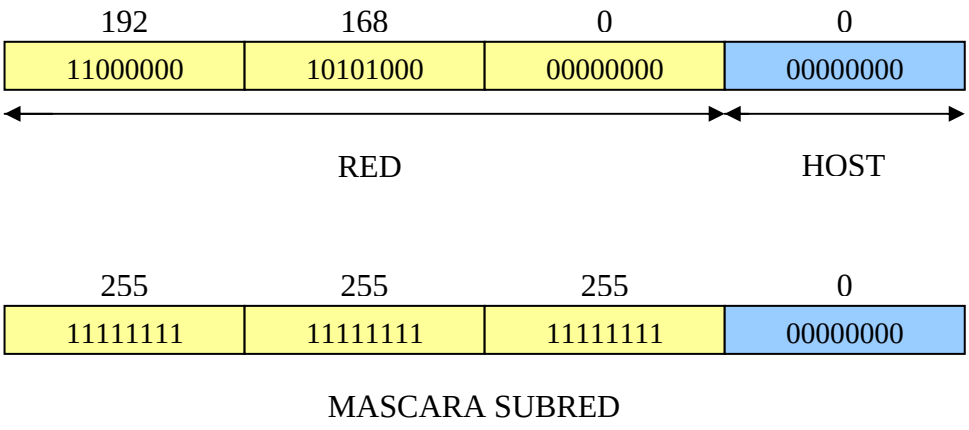


Figura 3.39. Esquema de Dirección de red y mascara de subred.

3.8.1 Distribución de direcciones IP

Esta distribución esta hecha de acuerdo a los servidores y access points con los que cuenta la red de la siguiente manera:

Direcciones para Servidores:

- Servidor Proxy 192.168.0.1
- Servidor de Dominio 192.168.0.2
- Servidor de correo 192.168.0.3
- Servidor de Antivirus 192.168.0.4
- Servidor de Aplicaciones 192.168.0.5
- Servidor de archivos 192.168.0.6
- Servidor de Impresoras 192.168.0.7
- Servidor Web. 192.168.0.8
- Servidor Radius 192.168.0.9

Direcciones para Access Points:

- Access point piso 0 192.168.0.10
- Access point piso 1 192.168.0.11
- Access point piso 2 192.168.0.12
- Access point piso 3 192.168.0.13
- Access point piso 4 192.168.0.14
- Access point piso 5 192.168.0.15
- Access point piso 6 192.168.0.16

Por cuestiones de diseño dejaremos reservadas 4 direcciones IP por si alguna vez se necesita agregar algún tipo de servidor a la red. Con estas consideraciones, las direcciones que serán asignadas a los computadores clientes serán desde 192.168.0.20 hasta 192.168.0.255 (235 host).

3.8.2 Direcciones de ISP

Las direcciones IP que asigna el proveedor de servicios de Internet (ISP) para la banda ancha de CABLEMODEM son:

IP	201.219.87.66
Mascara	255.255.255.248
Gateway	201.219.87.55

DNS1	200.63.221.1
DNS2	200.63.192.1

Estos datos serán utilizados en la configuración del servidor Proxy para distribuir el servicio de Internet a toda la red.

3.9 CONFIGURACIÓN DE EQUIPOS

En esta sección se presentarán todos los parámetros de configuración que tiene el access point de forma explicativa. En la siguiente sección se indicaran concretamente las configuraciones que se realizarán en cada equipo de acuerdo con el diseño desarrollado.

Para iniciar la configuración se debe acceder al menú de configuración por medio de un web browser, como el Internet Explorer de Windows, ingresando la dirección IP asignada por defecto al access point que es: 192.168.0.50, así:

Figura 3.40. Browser Internet Explorer 6.0.

Una vez ingresada esta dirección se accede al inicio de sesión del access point en la que se pide una contraseña de administrador para poder configurar el equipo, por defecto el equipo no tiene clave.

Figura 3.41. Inicio de sesión.

Al oprimir el botón “OK” ingresamos a la ventana principal de configuración en la que encontramos cinco pestañas de configuración que son: Inicio, Avanzados, Herramientas, Estado y Ayuda, cada una de ellas con diferentes parámetros de configuración del equipo las cuales se irán explicando una por una.

3.9.1 Inicio

En inicio hay 3 opciones que son: el asistente para configuración, inalámbrico y LAN como se muestra en la figura.

Asistente

El asistente para la configuración es una herramienta de ayuda para realizar configuraciones básicas por ese motivo no se explicara este punto.

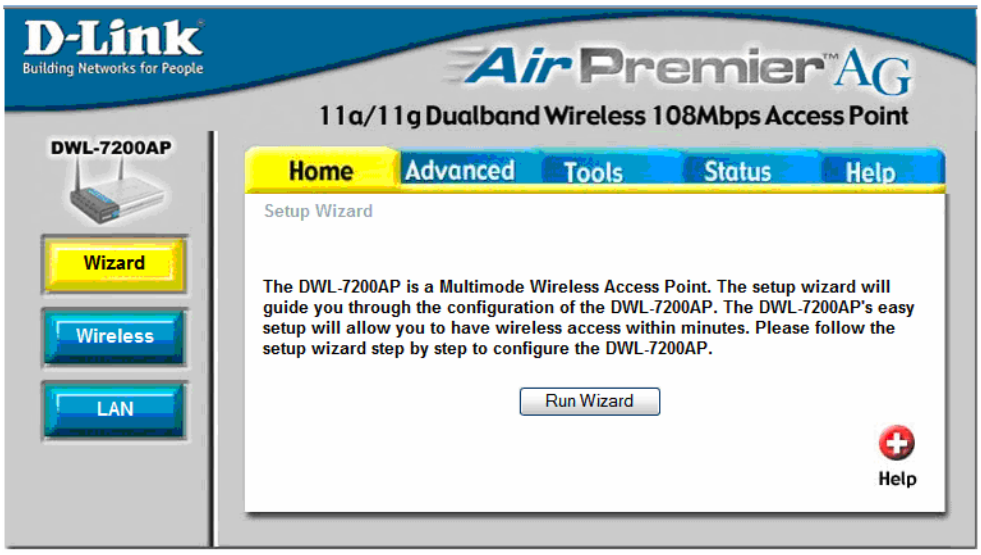


Figura 3.42. Menú Inicio – Asistente.

Inalámbrico

En esta parte se configura la banda inalámbrica, el SSID, la difusión de SSID broadcast y la asignación del canal.

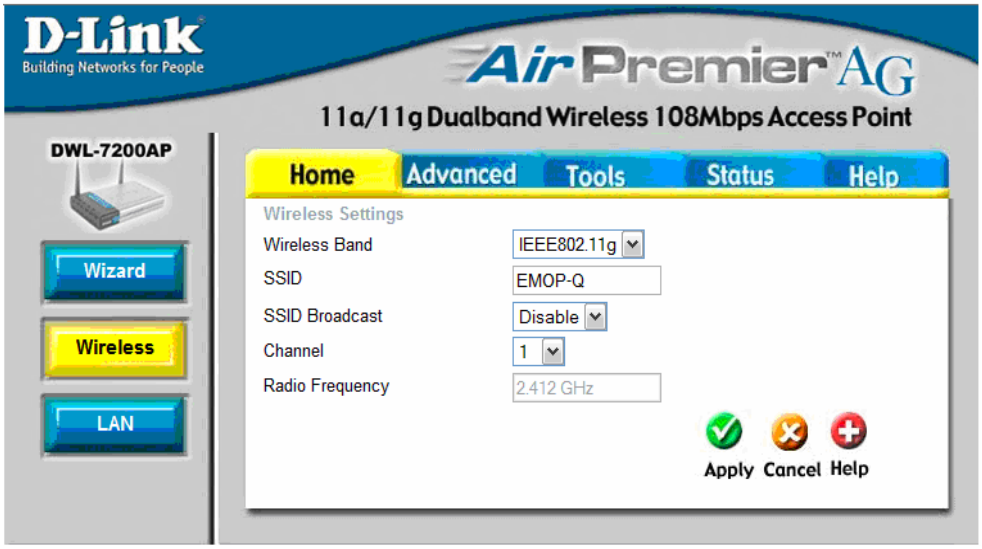


Figura 3.43. Menú Inicio – Inalámbrico.

Wireless Band es para seleccionar la banda en la que va a trabajar el access point, 802.11a u 802.11b/ (5 0 2.4 GHz). Se utilizará la banda de 2.4 GHz.

SSID es el nombre específico designado a la WLAN. El SSID es “EMOP-Q”. El SSID es igual para todos los access points.

SSID Broadcast es la difusión del SSID y es un modo de protección general. El SSID broadcast estará deshabilitado para ocultar el nombre de la red a usuarios no permitidos.

Channel es el canal de funcionamiento para el Access point, cada access point tendrá un canal distinto para evitar interferencias. En este caso es “1”.

LAN

En esta parte se configura la dirección IP del access point, la mascara de subred y la dirección de puerta de enlace (gateway).

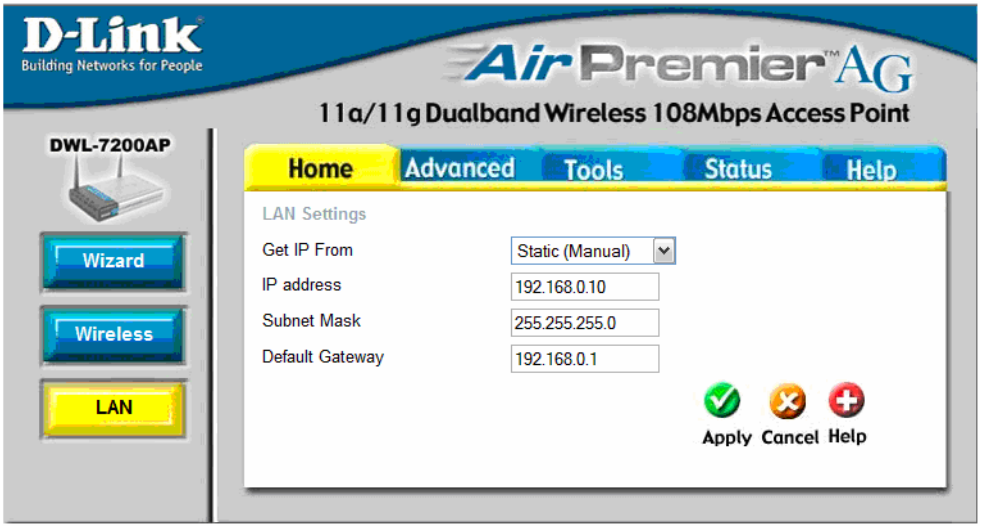


Figura 3.44. Menú Inicio – LAN.

Get IP from indica de donde se va a tomar la dirección IP para el access point, de un DHCP o de forma manual. Para este diseño se lo configura de forma estática (manual)

IP address es la dirección IP del primer access point que es: 192.168.0.10.

Subnet Mask es la mascara de subred, en este caso 255.255.255.0.

Default gateway es la puerta de enlace determinada por el que deben ir los paquetes (siguiente salto), lo configuramos con 192.168.0.1 (servidor proxy).

3.9.2 Avanzado

En Avanzado hay 6 opciones que son: Modo, rendimiento, filtros, Encriptación, Agrupación y servidor DHCP.

Modo

El modo indica la configuración de funcionamiento que se le da al access point. Este access point tiene 5 modos de funcionamiento.

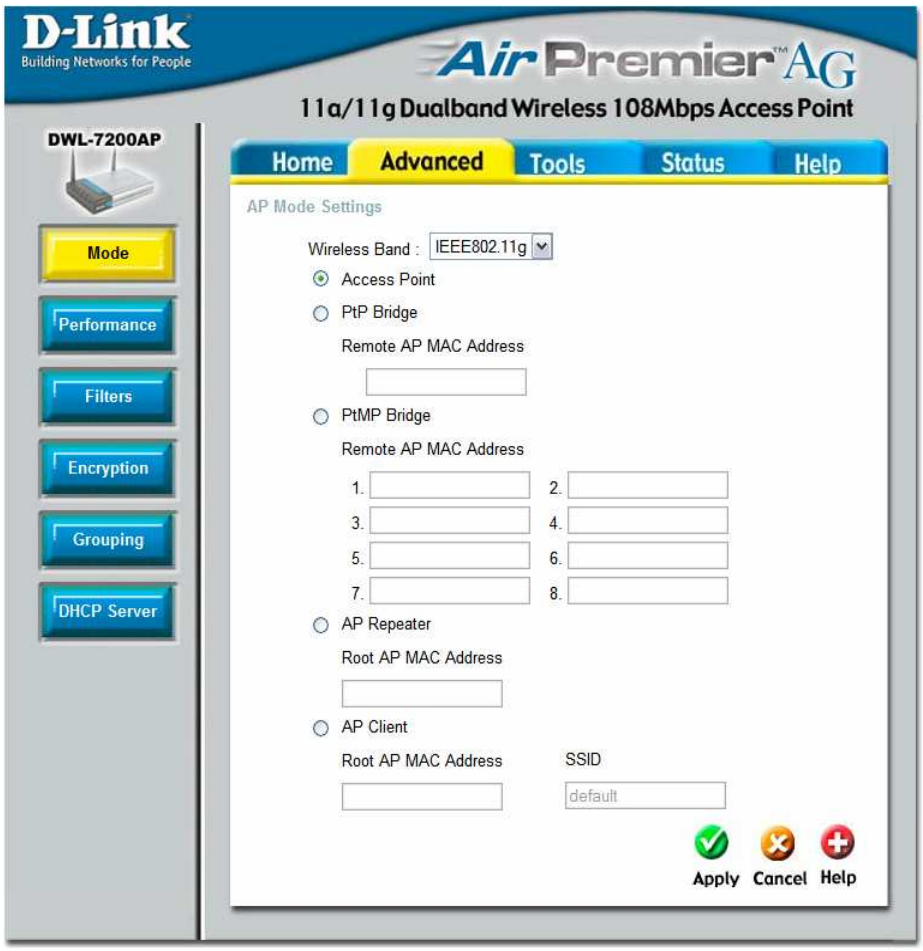


Figura 3.45. Menú Avanzado – Modo.

Access Point permite que el DWL-7200AP funcione como un punto de acceso inalámbrico para otros dispositivos inalámbricos se conectan a el.

PtP Bridge (point to point bridge) permite que el DWL-7200AP sea conectado a otro access point con capacidad de puenteo. Esto se utiliza para conectar redes inalámbricas como por ejemplo entre dos edificios.

PtMP Bridge (Point to Multiple Point Bridge) permite al DWL-7200AP conectarse con múltiples wireless access points que usen la función de puenteo. En este modo, se asociará con alguno o todos los bridges habilitados con sus direcciones MAC en la tabla de direcciones MAC del access point remoto.

AP Repeater permite que el DWL-7200AP funcione como repetidor. El repetidor extiende el rango de cobertura de radio de un access point específico. Se ingresa la dirección MAC en el access point remoto que requiere extender su cobertura.

AP Client permite que el DWL-7200AP funcione como un cliente wireless. En este modo, el usuario necesita ingresar el SSID del access point remoto para establecer una conexión. Al habilitar este modo se tiene la opción de usar “Site Survey” para escanear y conectarse a una red disponible. La dirección MAC será ingresada automáticamente cuando se use la herramienta Site Survey

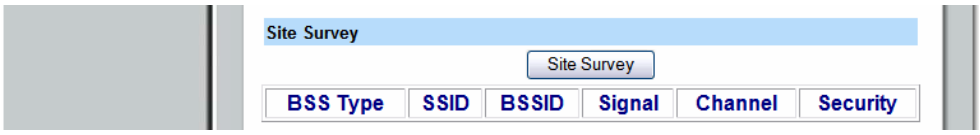


Figura 3.46. Menú Avanzado – Site Survey.

Rendimiento

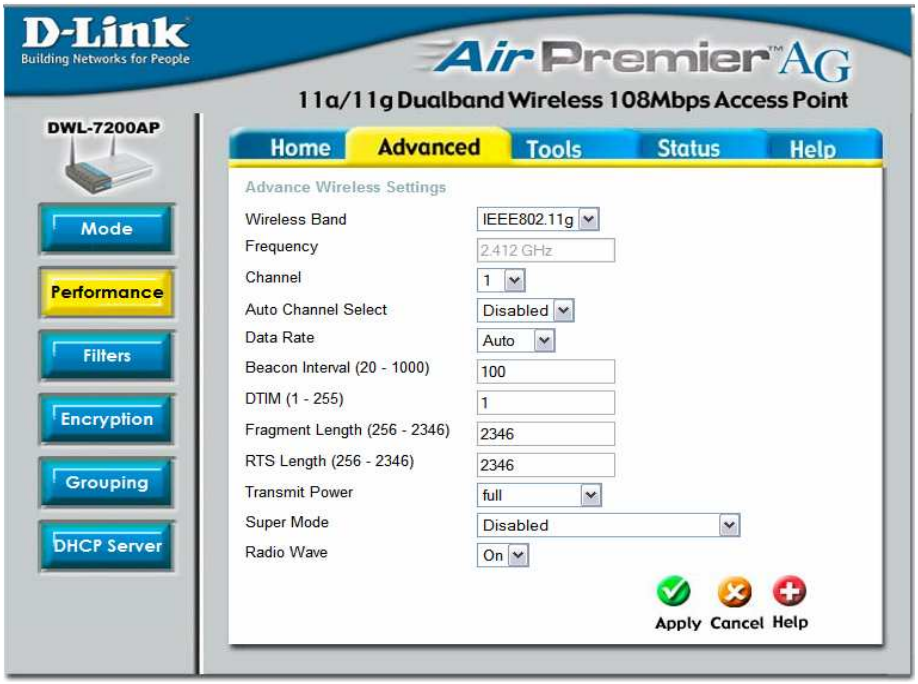


Figura 3.47. Menú Avanzado – Rendimiento.

Wireless Band selecciona la banda para configurar.

Frequency indica la frecuencia actual del access point. El valor depende del canal en q este configurado el access point. Este valor es solo información y no puede ser cambiado.

Channel indica el canal “seteado” en el access point. En este caso el canal es “1”. El canal puede ser cambiado para ajustar el canal en una red inalámbrica existente.

Auto Channel Select al habilitar esta sección el access point selecciona automáticamente el canal en el que se encuentre menos tráfico de información.

Data Rate Indica la tasa de transferencia de datos basada en la velocidad de los adaptadores inalámbricos que se encuentran en la red . El valor por defecto es “auto” y depende de los dispositivos conectados.

Beacon interval (200-1000) Beacons son paquetes enviados por el access point para sincronizar la red inalámbrica. El valor por defecto son 100 ms.

DTIM interval (1-255) es el rango para el mensaje de indicación de trafico de entrega (DTIM). DTIM es una cuenta regresiva que informa clientes de la próxima ventana para escuchar mensajes de broadcast y multicast.

Fragmentation Length (256-2346) Este valor debe permanecer en su valor por defecto (2346). Si se experimenta una alta tasa de error de paquetes, se puede aumentar ligeramente el valor de fragmentación.

RTS Length (256-2346) Este valor debe permanecer en su valor por defecto (2346). Si se encuentra inconsistencia de flujo de datos, solo se deber realizar modificaciones menores del valor de RTS.

Transmit Power la potencia de transmisión puede ser limitada por circunstancias donde la interferencia o el solapamiento de celdas afectan a la red. Las opciones de configuración son: full (default), half (-3dB), quarter (-6dB), eighth (-9dB) o min (minimo).

Super Setting El DWL-7200AP esta adherido al estándar IEEE 802.11a proveyendo tasas de transferencia inalámbricas altas sobre los 54 Mbps. Si se habilita el modo super setting el equipo es capaz de ofrecer velocidades superiores a los 72 Mbps.

Super Mode activa la opción de modo Super G. El valor por defecto es “desactivado”. El valor puede cambiarse de acuerdo a la capacidad de los dispositivos conectados. Las opciones que disponen son: Disabled, Super G without Turbo, Super G with Static Turbo y Super G with Dynamic Turbo.

Radio Wave indica la configuración de aparato de radio. Por defecto es encendido “On”.

Filtros

El access point DWL-7200AP puede ser configurado para admitir o denegar el acceso a clientes wireless por medio de una lista de direcciones MAC.

Wireless Access Settings

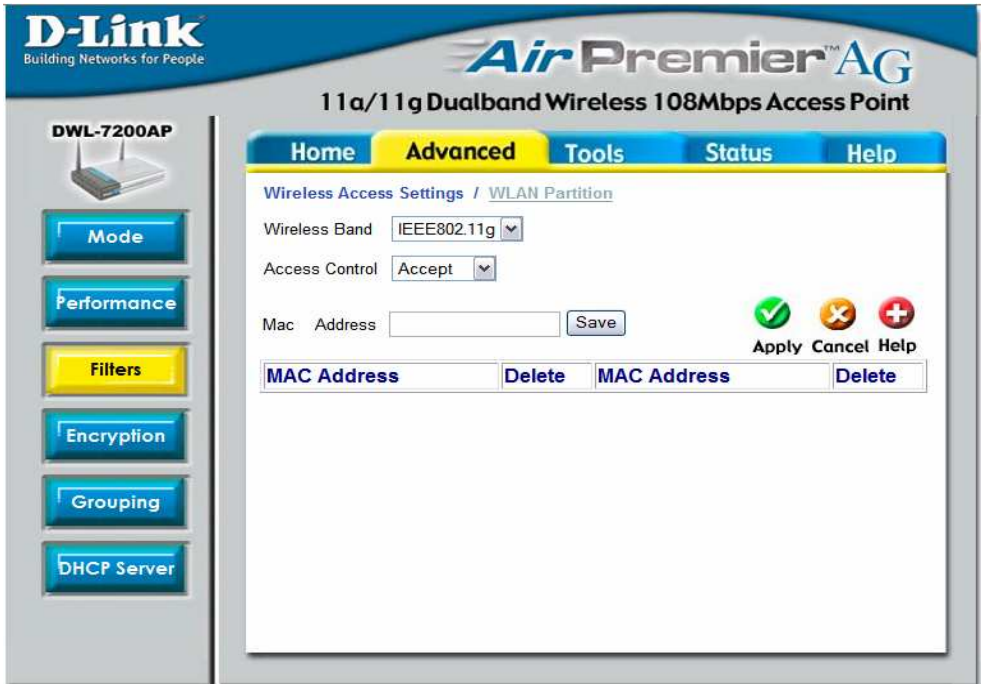


Figura 3.48. Menú Avanzado – Filtros – Wireless access settings.

Wireless Band selecciona la banda de frecuencias para configurar.

Access Control usa las direcciones MAC de los clientes para autorizar el acceso a la red por medio del access point. Se selecciona Accept para habilitar la comunicación entre el access point y otros dispositivos inalámbricos que estén en la lista de direcciones MAC. Se selecciona Reject para el caso contrario.

Mac Address es el cuadro de texto por el que se van ingresando las direcciones MAC que van a estar en la lista para filtrado.

WLAN Partition

Figura 3.49. Menú Avanzado – Filtros – WLAN partition.

Wireless Band selecciona la banda de frecuencias para configurar.

Internal Station Connection cuando esto está activado no hay barrera entre la comunicación de estaciones inalámbricas que se conectan al punto de acceso. Si esta desactivado, las estaciones inalámbricas seleccionadas en una de las bandas no están permitidas completamente para intercambiar datos con el access point.

Ethernet to WLAN Access cuando esto está activado no hay barrera entre el flujo de datos desde ethernet hacia los dispositivos inalámbricos conectados en el access point. Si esta desactivado, todos los datos desde ethernet son bloqueados, los dispositivos inalámbricos no pueden enviar datos a la ethernet.

Connection Between 802.11a & 802.11g cuando esto está activado, los dispositivos 802.11a de la red son habilitados para intercambiar información con

los dispositivos 802.11g. Si está desactivado, se crea una partición de la red entre los equipos 802.11 a y g y no se permite transmitir información entre ellos.

Encriptación

Wireless Band selecciona la banda de frecuencias para configurar.

Authentication Para agregar seguridad a la red inalámbrica debe estar habilitada la encriptación de datos. El access point presenta cuatro tipos de autenticación que son: open system, shared key, open system/shared key y WPA.

- ***Open system*** Para este tipo de autenticación el access point es visible para todos los dispositivos de la red y conectarse a él es simple ya q no solicita ninguna clave de autenticación.
- ***Shared key*** Para este tipo de autenticación el access point no es visible para todos los dispositivos de la red, únicamente se podrán conectar los dispositivos que compartan la misma clave WEP que puede ser de 64, 128 y 152 bits. El access point permite ingresar 4 claves WEP (Key Table) y una casilla (Valid Key) que permite seleccionar una de las 4 claves para que sea válida.
- ***system/shared key*** Es una combinación de las dos autenticaciones anteriores, la única variación es que se permite habilitar o deshabilitar la encriptación según la necesidad del usuario.
- ***WPA*** Soporta 2 protocolos de administración de autenticación por clave en modo de infraestructura usando 802.11x que son: PSK y con EAP. El modo PSK soporta directamente una clave compartida como encriptación (sin protocolo administrador). El modo EAP soporta un protocolo administrador, es decir se utiliza un servidor de autenticación Radius).

PassPhrase Es la frase de paso cuando se utiliza WPA-PSK.

Cipher Type Cuando se utiliza EAP se puede escoger el tipo de cifrado entre AES, auto o TKIP.

Radius Server Se ingresa la dirección IP del servidor Radius (WPA-EAP). La dirección asignada al servidor radius es la 192.168.0.9

Group key Update Interval se escoge el intervalo durante en cual la clave de grupo será válida. El valor por defecto de 1800 es recomendado.

Radius Port Es el puerto de comunicación por el cual funcionará el servidor radius, esto es configurado en el access point y en el servidor.

Radius secret Es el nombre del servidor radius.

Key Type Se puede ingresar las claves de encriptación de modo hexadecimal o ASCII.

Figura 3.50. Menú Avanzado – Encriptación.

Servidor DHCP

El servidor DHCP (Dynamic Host Control Protocol) asigna direcciones IP de forma dinámica cuando un host inalámbrico es encendido y requiere una dirección IP para conectarse a la red. DHCP es inhabilitado por defecto en el access point.

Dynamic Pool Settings

Dynamic pool permite, a los clientes inalámbricos, recibir una dirección IP disponible al momento de la conexión. Las IP´s disponibles son definidas mediante configuraciones que son compatibles con la red existente o con la configuración de una nueva red.

Function Enable/Disable en ese punto se habilitará o deshabilitará la configuración “dynamic pool”. El valor por defecto es "Disabled".

IP Assigned From Este es la dirección de inicio del rango de direcciones IP disponibles para los dispositivos clientes.

The Range of Pool (1-255) Este es el rango o número de direcciones IP que estarán disponibles por el servidor DHCP. El rango de direcciones IP dependerá de la dirección asignada en “IP Assigned from” a partir de esa dirección se habilitará el rango.

SubMask Se ingresa la mascara de subred de la dirección ingresada en “IP Assigned from”.

Gateway Se ingresa la dirección de gateway de la red existente o de la nueva red.

Wins Se ingresa la dirección Wins (Windows Internet Naming Service) de la red existente o de la nueva red.

DNS Se ingresa la dirección DNS (Domain Name Server) de la red existente o de la nueva red.

Domain Name Se ingresa el nombre de dominio de la red existente o de la nueva red.

Lease Time Se ingresa la longitud del tiempo para el arrendamiento de la dirección IP al cliente dispositivo.

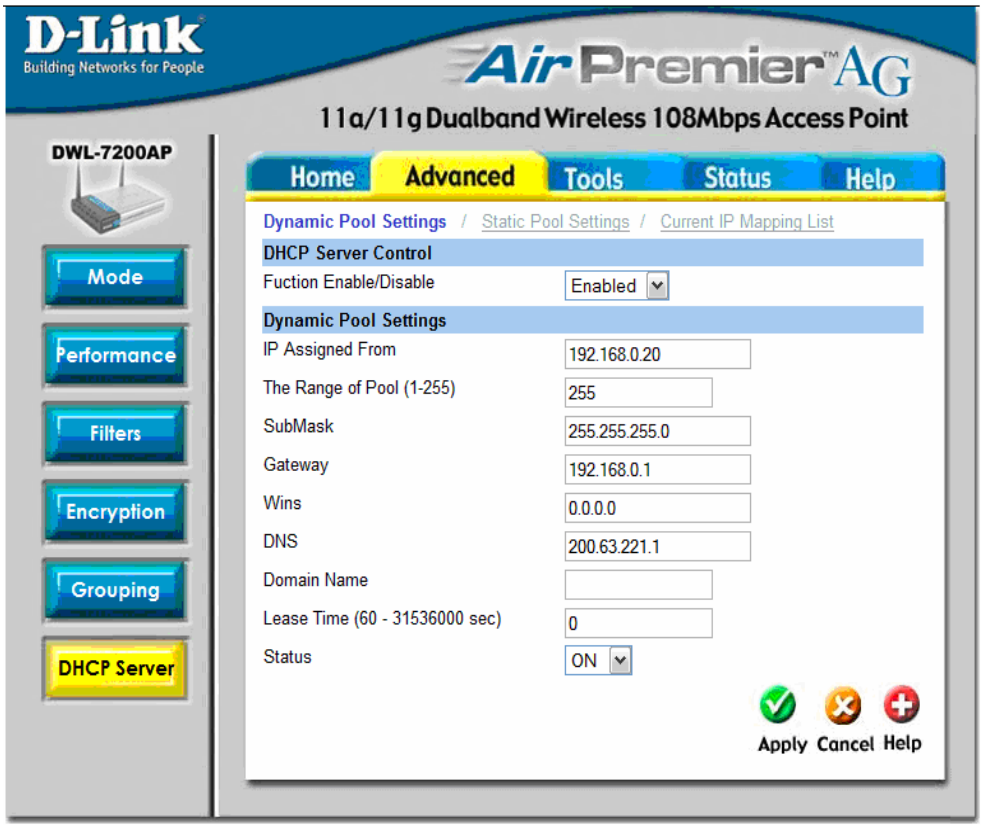


Figura 3.51. Menú Avanzado – DHCP server.

Static Pool Settings

En este punto se realizan configuraciones estáticas del servidor DHCP, es decir, no se utiliza la asignación dinámica de direcciones IP para los host sino que se ingresa de forma manual para cada host registrando la dirección MAC de la tarjeta de red.

Function Enable/Disable en ese punto se habilitará o deshabilitará la configuración “dynamic pool”. El valor por defecto es "Disabled".

Assigned IP Se ingresa la dirección IP que es asignada por la dirección MAC. Ingresada en “Assigned MAC Address”.

Assigned MAC Address Se ingresa la dirección MAC del equipo cliente que requiere una dirección IP.

Los siguientes parámetros, subMask, Gateway, Wins, DNS, y Domain Name son configurados de la misma forma que en “Dynamic Pool Settings”.

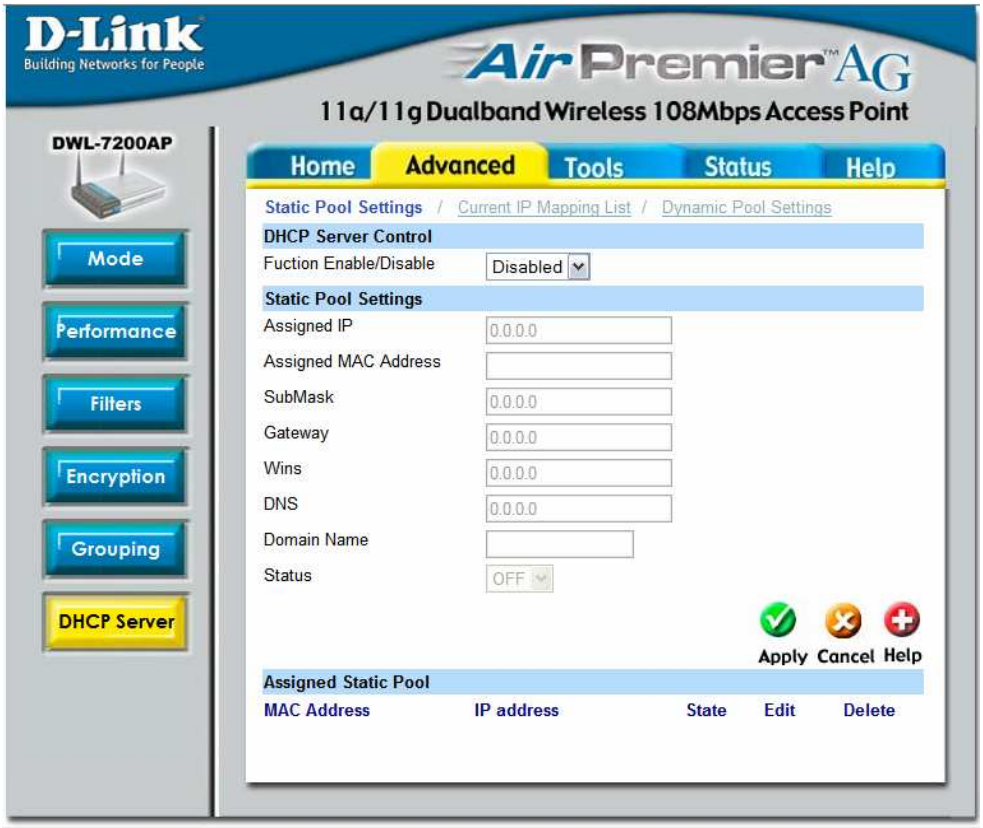


Figura 3.52. Menú Avanzado – DHCP Server.

Current IP Mapping List

Las computadoras clientes de DCHP conectadas al access point tendrán su información visualizada en la tabla “DHCP Dynamic/Static”. Esta tabla indicará la dirección MAC, la dirección IP, el tiempo de “arriendo” de DHCP de cada dispositivo cliente.

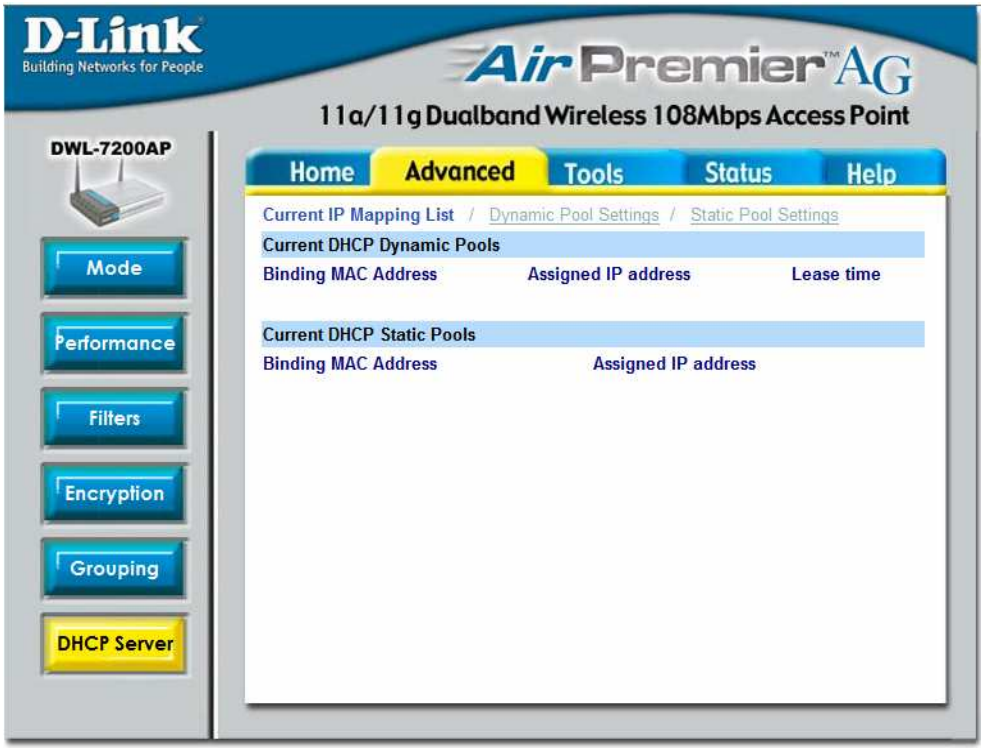


Figura 3.53. Menú Avanzado – DHCP server.

3.9.3 Herramientas

Aquí encontramos configuraciones básicas para el access point como son: administración, sistema, firmware, configuración de archivo y misceláneo.

Administración

Se ingresan contraseñas a la sesión de administrador y usuario para restringir el acceso al menú de configuración a personas ajenas. También se puede activar la administración remota por medio de un puerto de acceso.

(SIGUIENTE HOJA)

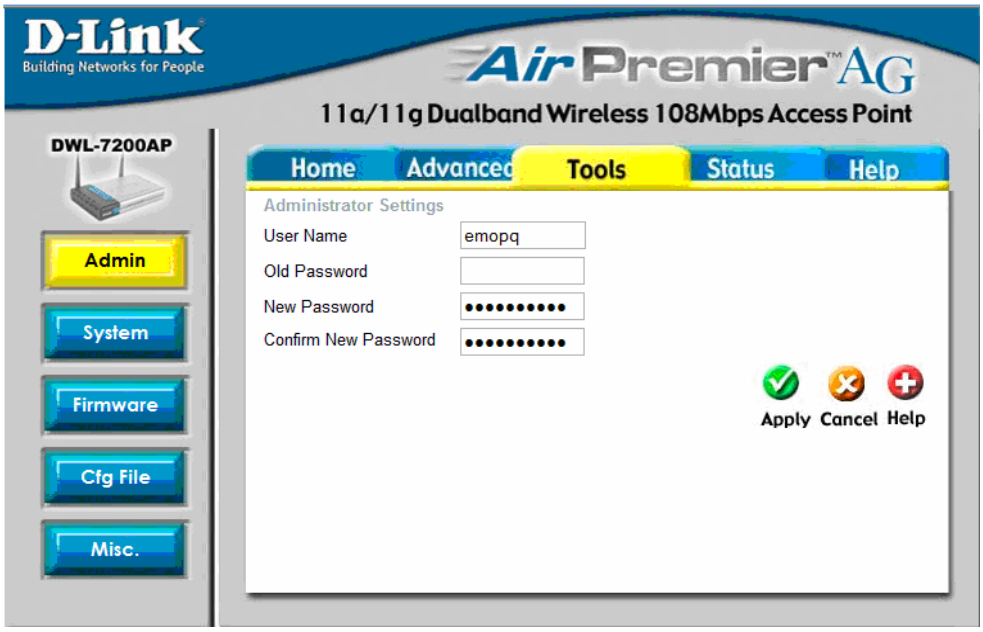


Figura 3.54. Menú Herramientas – Administración.

Sistema

El sistemas de puede reiniciar el equipo vía software y recuperar las configuraciones de fábrica.

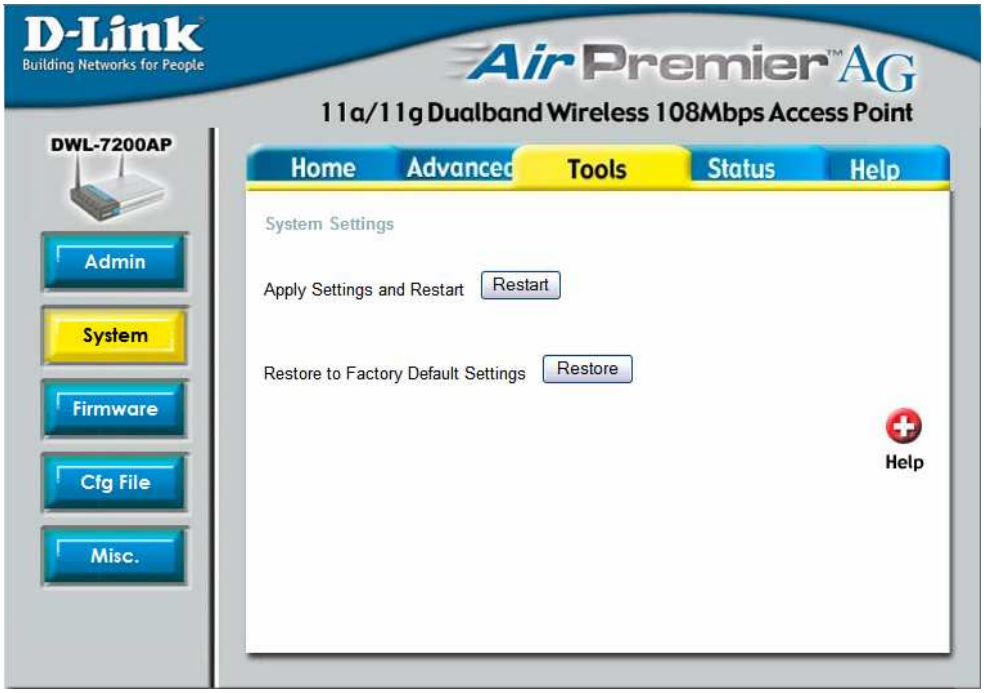


Figura 3.55. Menú Herramientas – Sistema.

Apply Settings and Restart se utiliza para “resetear” (inicializar) el access point con las configuraciones en curso.

Restore Default Settings se utiliza pare restaurar las configuraciones de fabricación del access point.

Firmware

El firmware del equipo puede ser actualizado para resolver cualquier conflicto de sistema o compatibilidad. Se debe visitar la pagina www.dlink.com para descargar la última versión del firmware de este dispositivo.

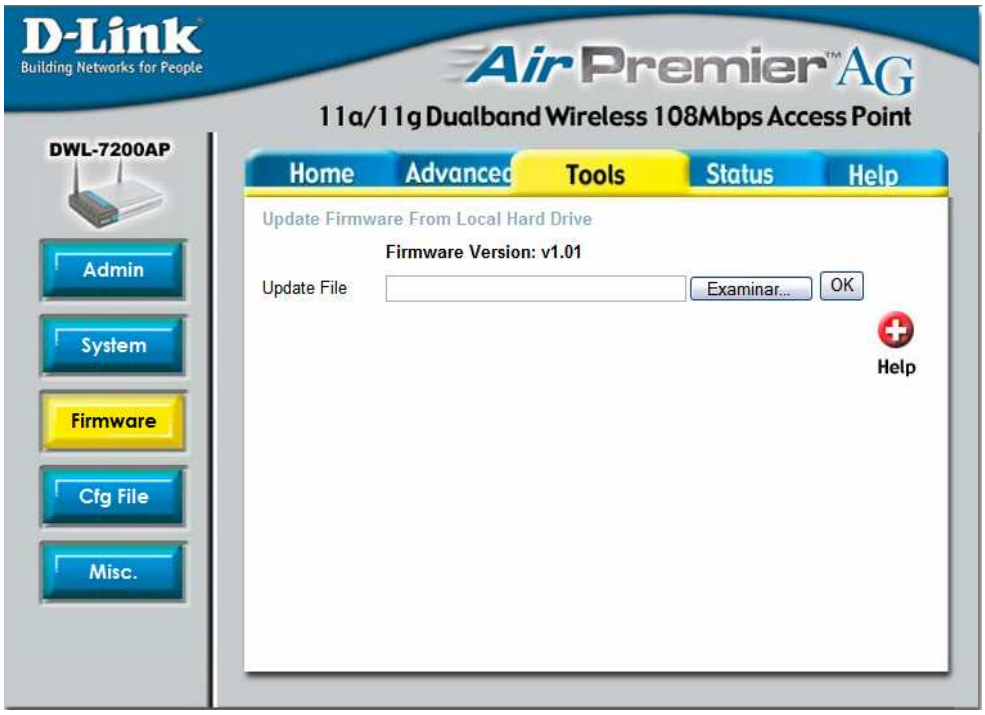


Figura 3.56. Menú Herramientas – Firmware.

Update firmware From Local Hard Drive se utiliza para actualizar el equipo con el último firmware descargado al disco local. Se busca el archivo oprimiendo “EXAMINAR” y luego pulsando “OK”.

Configuración de archivo

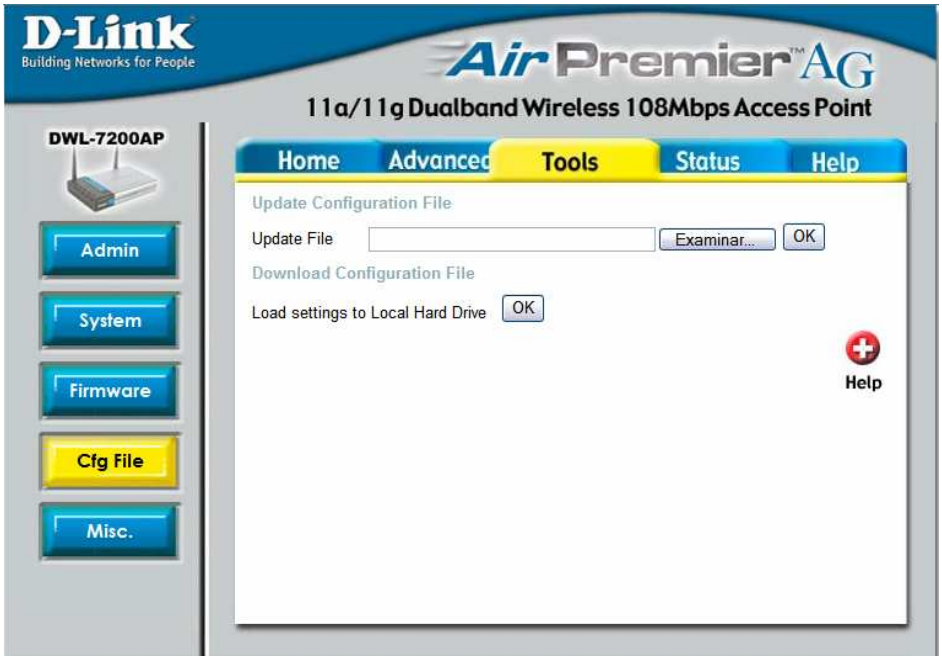


Figura 3.57. Menú Herramientas – Configuración de archivo.

Se utiliza esta opción para guardar en disco un archivo con extensión .gws con todas las configuraciones realizadas a manera de backup.

Misceláneo

El menú misceláneo es usado para configurar el Telnet en el access point.

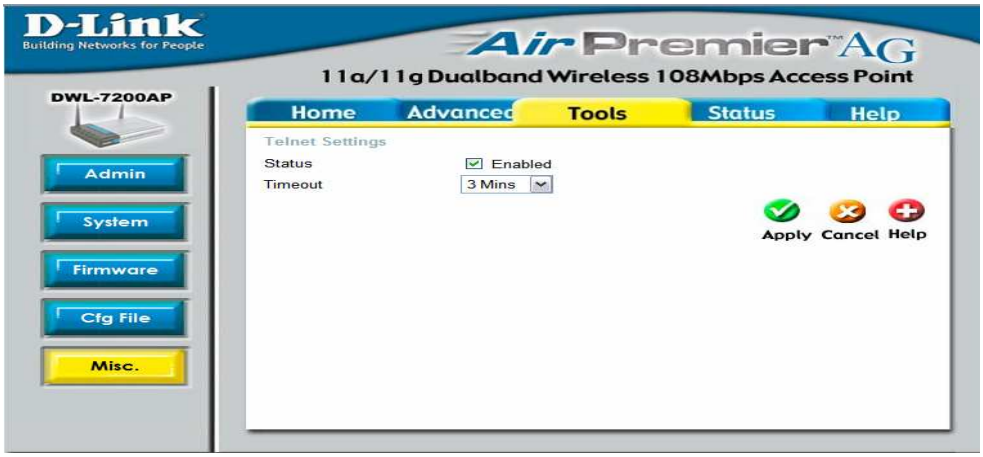


Figura 3.58. Menú Herramientas – Misceláneo.

Status sirve para habilitar o deshabilitar la opción de telnet.

Timeout es el tiempo muerto del telnet y esta configurado en 3 minutos.

3.9.4 Estado

Información del dispositivo

Esta pantalla muestra la información actual del access point. La información mostrada es la versión del firmware que está corriendo actualmente.

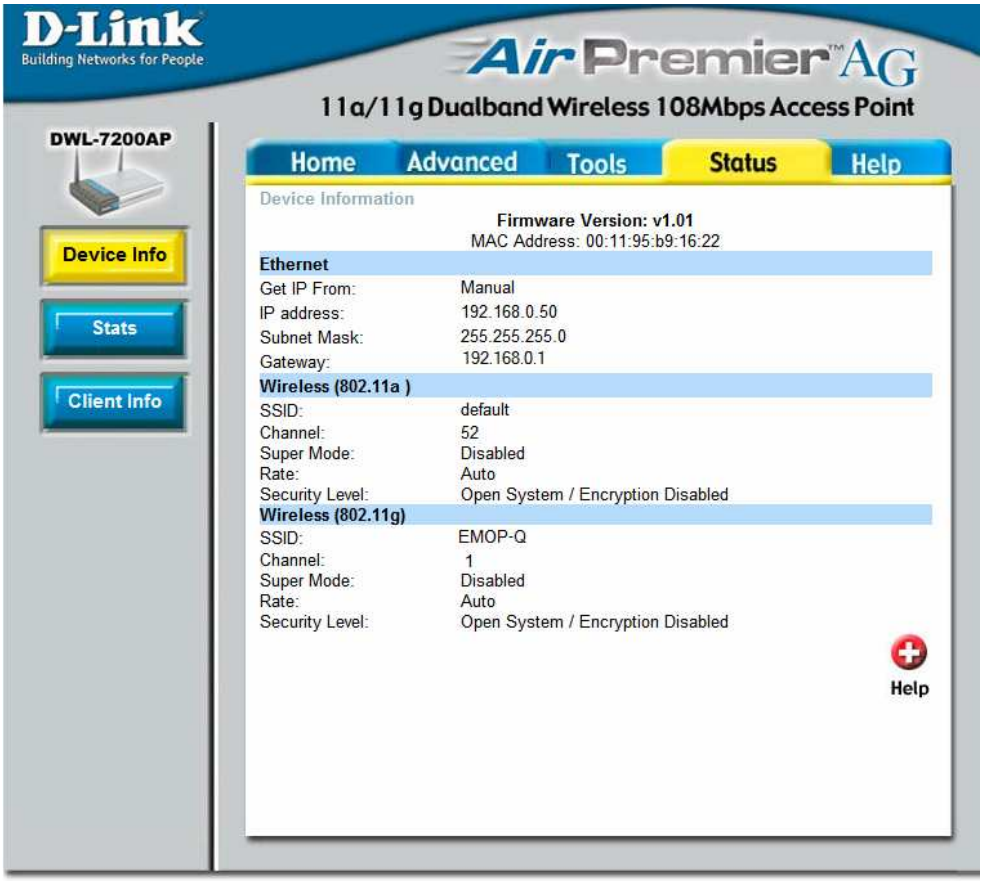


Figura 3.59. Menú Estado – Información del dispositivo.

Como podemos ver, se muestra la información general del dispositivo como son los parámetros ethernet y los parámetros de 802.11a y 802.11g.

En los parámetros de ethernet se muestra la dirección IP, la mascara de subred y el gateway del access point. En los parámetros 802.11a y g se muestra el SSID, el canal asignado, super mode, tasa de transmisión, nivel de seguridad.

Estadísticas

En esta parte se muestra las estadísticas de tráfico de la red para los paquetes de transmisión y recepción tanto en el puerto ethernet como en las conexiones inalámbricas asociadas al access point. Estas estadísticas son realizadas para el modo 802.11ª y 802.11g dependiendo de la banda de frecuencias que se esté utilizando.

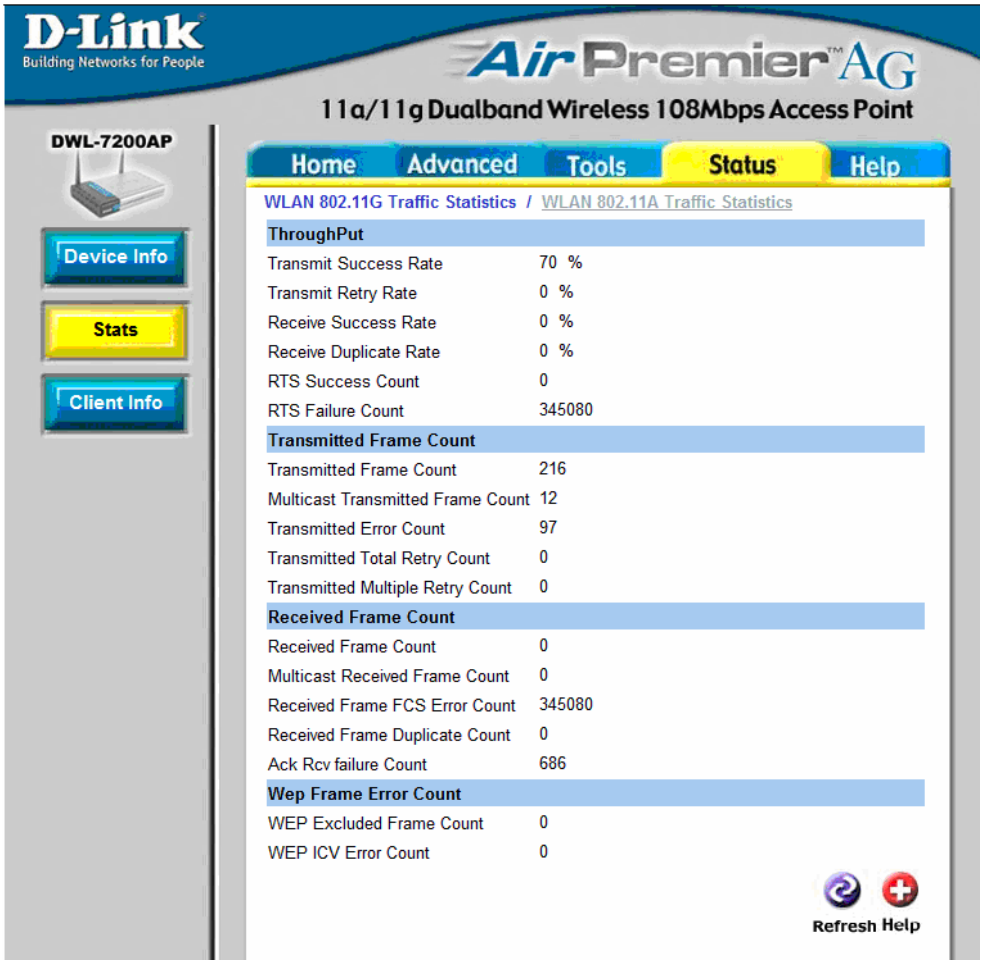


Figura 3.60. Menú Estado – Estadísticas.

Información de Cliente

Aquí se muestra la información de los clientes q están actualmente conectados al access point.

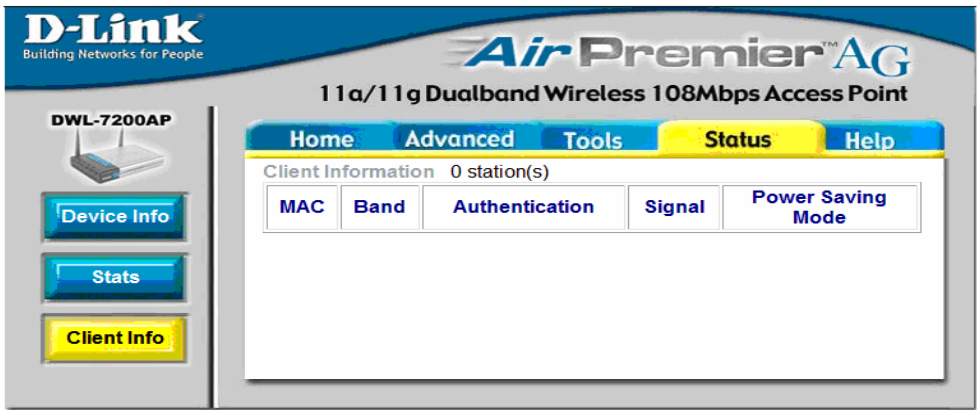


Figura 3.61 Menú Estado – Información del cliente.

3.9.5 Ayuda

Es un listado de todos los parámetros de configuración que posee el access point con su respectiva explicación.

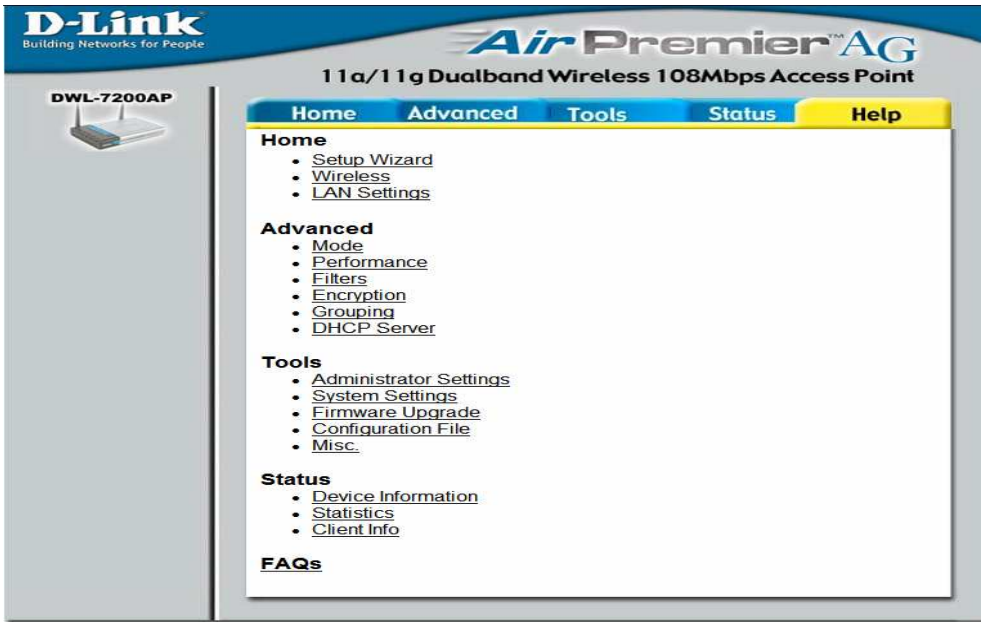


Figura 3.62. Menú Ayuda.

3.10 SEGURIDAD

3.10.1 Servidor Radius.

RADIUS (Remote Access Dial-In User Servise) es el protocolo más utilizado para autorizar acceso a redes. Este es un protocolo de autenticación y autorización para aplicaciones de acceso a la red inalámbrica, este acceso debe ser autorizado para cada uno de los clientes inalámbricos de la red.

Al momento de realizar una conexión de un host a la red el cliente envía una información que generalmente es un nombre de usuario y una contraseña. Esta información es enviada al servidor Radius (sobre el protocolo Radius) el cual comprueba, en su base de datos, que la información es correcta usando esquemas de autentificación como en EAP (Extensible Authentication Protocol). Si es aceptado, el servidor autorizará el acceso a la red y le asignará recursos de red como la dirección IP, el acceso a Internet, etc.

La autenticación esta dada por la comparación de las credenciales (usuario y contraseña) entre el mensaje de requerimiento de acceso y los datos almacenados en la base de datos del Radius. En resumen, el servidor Radius realizará las siguientes acciones al momento de autorizar el acceso a la red a un cliente.

1. El autenticador envía un paquete de "EAP-Request/Identity" al suplicante tan pronto como detecte que el acoplamiento es activo.
2. El suplicante envía un paquete de "EAP-Response/Identity" al autenticador, que pasa directamente al servidor de la autenticación.
3. El servidor de la autenticación envía un desafío al autenticador. El autenticador desempaqueta el contenido del paquete, lo empaqueta de nuevo en EAPOL y lo envía al suplicante.
4. El suplicante responde al desafío vía el autenticador y pasa la respuesta al servidor de autenticación.

5. Si el suplicante proporciona identidad apropiada, el servidor de autenticación responde con un mensaje de éxito al autenticador, que es pasado así mismo al suplicante. El autenticador permite a partir de este momento el acceso al suplicante.

El siguiente gráfico explica con más detalle todo el proceso de autenticación que realizará el servidor radius junto con el access point.

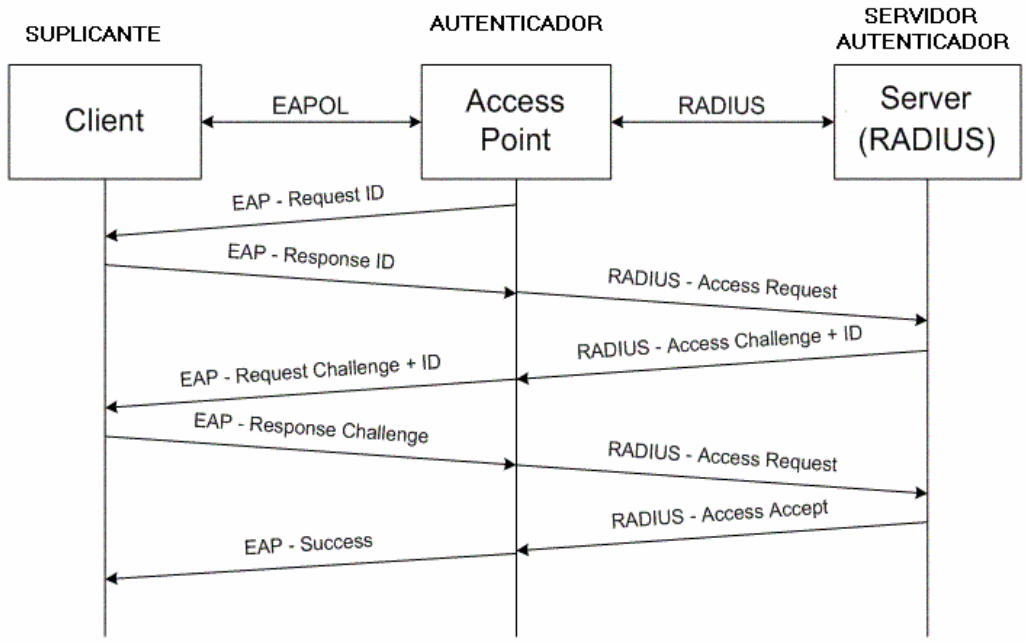


Figura 3.63. Esquema de funcionamiento de Radius.

Para realizar la implementación del servidor radius se necesita como sistema operativo la plataforma LINUX y como software se puede utilizar FREERADIUS que se lo puede obtener de www.freeradius.org. Los servidores radius trabajen en el puerto 1812, necesitan una dirección IP y un nombre para el servidor (Radius Secret), estos parámetros serán configurados en cada access point.

Existen en el mercado sitios web que ofrecen servidores radius y servicios de instalación, configuración y mantenimiento. Las características de los servidores son diferentes dependiendo del proveedor radius.

3.11 RESUMEN DE CONFIGURACIONES.

Como se indicó en los mapas de cobertura, el diseño tiene 7 access points (uno en cada piso del edificio) a los cuales ya se les asignaron una dirección IP y se les asignará también un canal de acuerdo a la explicación que se indico al comienzo del capitulo para evitar interferencias.

El siguiente listado indica todas las configuraciones que se realizarán a los equipos de acuerdo al esquema que se ha presentado y a los estudios de cobertura, seguridad y direccionamiento IP que se han realizado en este proyecto.

HOME

En esta sección existen parámetros que son comunes para todos los equipos como son:

- Banda de funcionamiento. 802.11g
- SSID. EMOP-Q
- SSID broadcast. Disable.
- Get IP from. Static (manual)

El siguiente cuadro muestra las configuraciones para de cada access point.

Access Point	Canal	Dirección IP	Mascara	Gateway
Piso 0	1	192.168.0.10	255.255.255.0	192.168.0.1
Piso 1	4	192.168.0.11	255.255.255.0	192.168.0.1
Piso 2	7	192.168.0.12	255.255.255.0	192.168.0.1
Piso 3	11	192.168.0.13	255.255.255.0	192.168.0.1
Piso 4	1	192.168.0.14	255.255.255.0	192.168.0.1
Piso 5	4	192.168.0.15	255.255.255.0	192.168.0.1
Piso 6	7	192.168.0.16	255.255.255.0	192.168.0.1

Tabla 3.3. Configuraciones de access points.

ADVANCED

Los parámetros de configuración son comunes para todos los equipos.

Modo

- Banda de funcionamiento. 802.11g
- AP Modo. Access Point

Performance

- Banda de funcionamiento. 802.11g
- Canal. (Asignado a cada access point)
- Selección Auto canal. Disable
- Velocidad de datos. Auto
- Potencia de transmisión. Full
- Super mode. Disable

Filtros

- Banda de funcionamiento. 802.11g
- Control de accesso. Accept

Encriptación

- Banda de funcionamiento. 802.11g
- Autenticación. WPA-EAP
- Cipher Type. Auto
- Radius Server. 192.168.0.9
- Radius port. 1812
- Radius secret. RADIUSEMOPQ

DHCP Server

Como el área de administración de la red se encuentra en el tercer piso, el access point del tercer piso será el encargado de actuar como servidor de DHCP por lo cual se lo configurará para que asigne las direcciones IP en forma dinámica y al resto de access points se les deshabilitará el DHCP de la siguiente manera:

Dinamic Pool Settings

Access Point	Dirección IP
Piso 0	DISABLED
Piso 1	DISABLED
Piso 2	DISABLED
Piso 3	ENABLED
Piso 4	DISABLED
Piso 5	DISABLED
Piso 6	DISABLED

Tabla 3.4. Configuraciones de direcciones IP para access points..

Para que el access point del tercer piso sea el que actúa como servidor DHCP se debe realizar las siguientes configuraciones extras.

Dinamic Pool Settings

- IP asignada desde. 192.168.0.20
- Rango de IP´s. 255
- Mascara de subred. 255.255.255.0
- Gateway. 192.168.0.1

3.12 CONFIGURACIÓN DE ADAPTADORES INALÁMBRICOS

Los adaptadores inalámbricos que se usaran en este diseño son los DWL-AG132 de la línea Air Premier de D-Link. Estos son uno de los adaptadores que son compatibles con el Access point DWL-7200AP.

3.12.1 Características

A continuación se muestra un gráfico del adaptador inalámbrico USB con su base de extensión incluida.

Figura 3.64. Adaptador DWL- AG132.

El adaptador inalámbrico USB DWL-AG132 presenta las siguientes características.

- Tamaño compacto para ubicarlo en cualquier lugar.
- Conveniente instalación Plug & Play.
- Totalmente compatible con 802.11b y g.
- Alimentado por el puerto USB, no necesita puente de energía externa.
- Estándar USB 2.0.
- Mayor seguridad utilizando 802.1X y WPA.
- Provee una señal inalámbrica con velocidad de transferencia de hasta 108 Mbps en el modo Turbo.
- Óptima recepción wireless. Se incluye un soporte con una extensión USB para posicionar de mejor manera el equipo.
- Soporta redes con infraestructura que utilizan Access points.

3.12.2 Configuración del equipo

El adaptador inalámbrico incluye en un CD un utilitario para instalación que es de fácil manejo ya que indica paso a paso como instalar el adaptador en una computadora, a demás, al ser Plug & Play se hace más fácil su instalación. Por ese motivo se obviará este paso y entraremos directamente a la configuración para conectarse a la red.

Una vez instalado el adaptador, el utilitario hace un escaneo del sector para ver si se encuentra alguna red inalámbrica disponible. El utilitario presenta la siguiente pantalla principal.

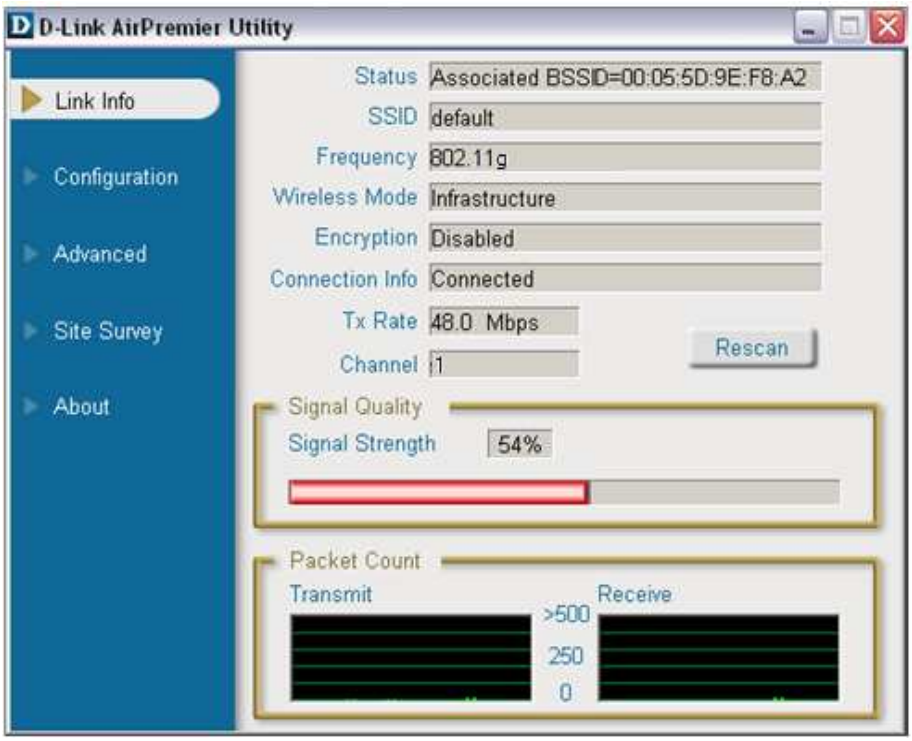


Figura 3.65. Utilitario del DWL- AG132.

Seleccionamos la pestaña “Configuration” para introducir los parámetros con los cuales podremos ingresar a la red EMOP-Q. En esta pantalla se introducirán los siguientes parámetros:

- SSID EMOP-Q.
- Wireless Mode INFRAESTRUCTURE.
- Data Encryption DISABLED.
- Authentication AUTO.

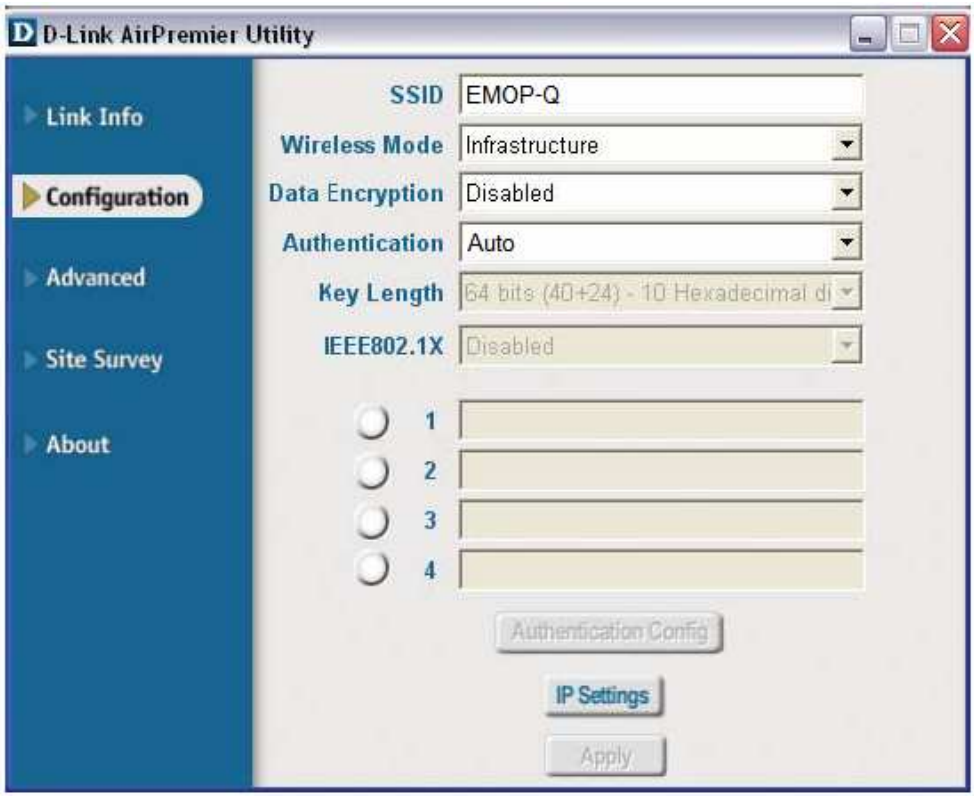


Figura 3.66. Configuración DWL- AG132.

El botón “IP Settings” sirve para configurar la dirección del adaptador, Como la red EMOP-Q tiene un servidor DCHP las direcciones IP y DNS serán asignadas de forma automática a cada adaptador por lo que la configuración debe ser “Obtain an IP Address Automatically” (obtener dirección Ip automáticamente) y “Obtain DNS server Address Automatically”.

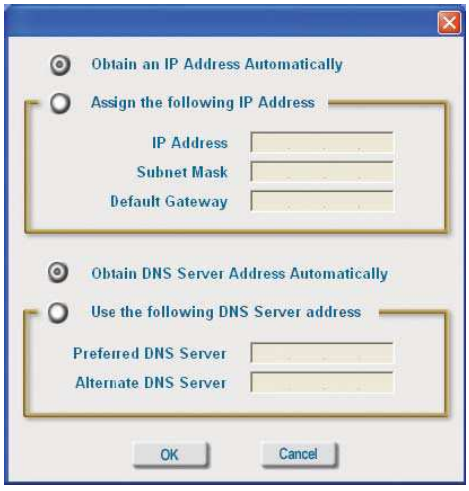


Figura 3.67. Configuración de direcciones IP y DNS.

Con esta configuración el adaptador reconocerá a la red EMOP-Q pero no podrá conectarse hasta no realizar las configuraciones avanzadas para que el servidor Radius lo reconozca. Para configurar esto, seleccionamos la pestaña “Site Survey” en la cual se configura el adaptador para que sea reconocido.

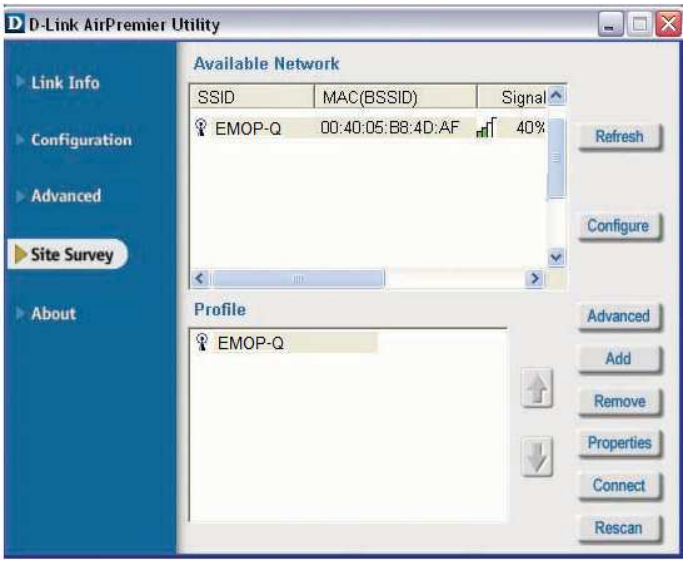


Figura 3.68. Site Survey.

Como se puede observar, la red EMOP-Q está reconocida por el adaptador pero todavía no esta conectado. Par esto, se selecciona el botón “Configure” y entramos a la siguiente pantalla y en “authentication” seleccionamos WPA.

Figura 3.69. Site Survey - Configure.

El siguiente paso es “Authentication Config” donde se selecciona el modo EAP, en este caso será EAP-TLS Y también el nombre de usuario, luego de esto aparece una ventana en la que se ingresa la dirección IP del servidor radius. Y con esto esta listo en adaptador para conectarse a la red.

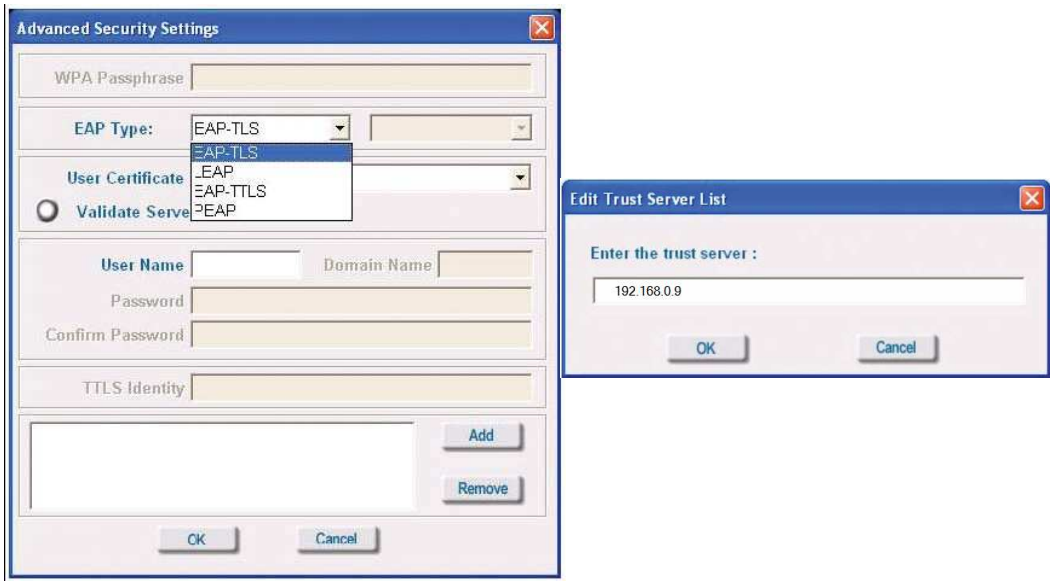


Figura 3.70. Configuración de seguridad avanzada.

3.13 DISEÑO DE LA RED INALÁMBRICA

Con la solución presentada en los puntos anteriores se ha realizado el esquema de la nueva red WLAN como muestra la figura.

(SIGUIENTE HOJA)

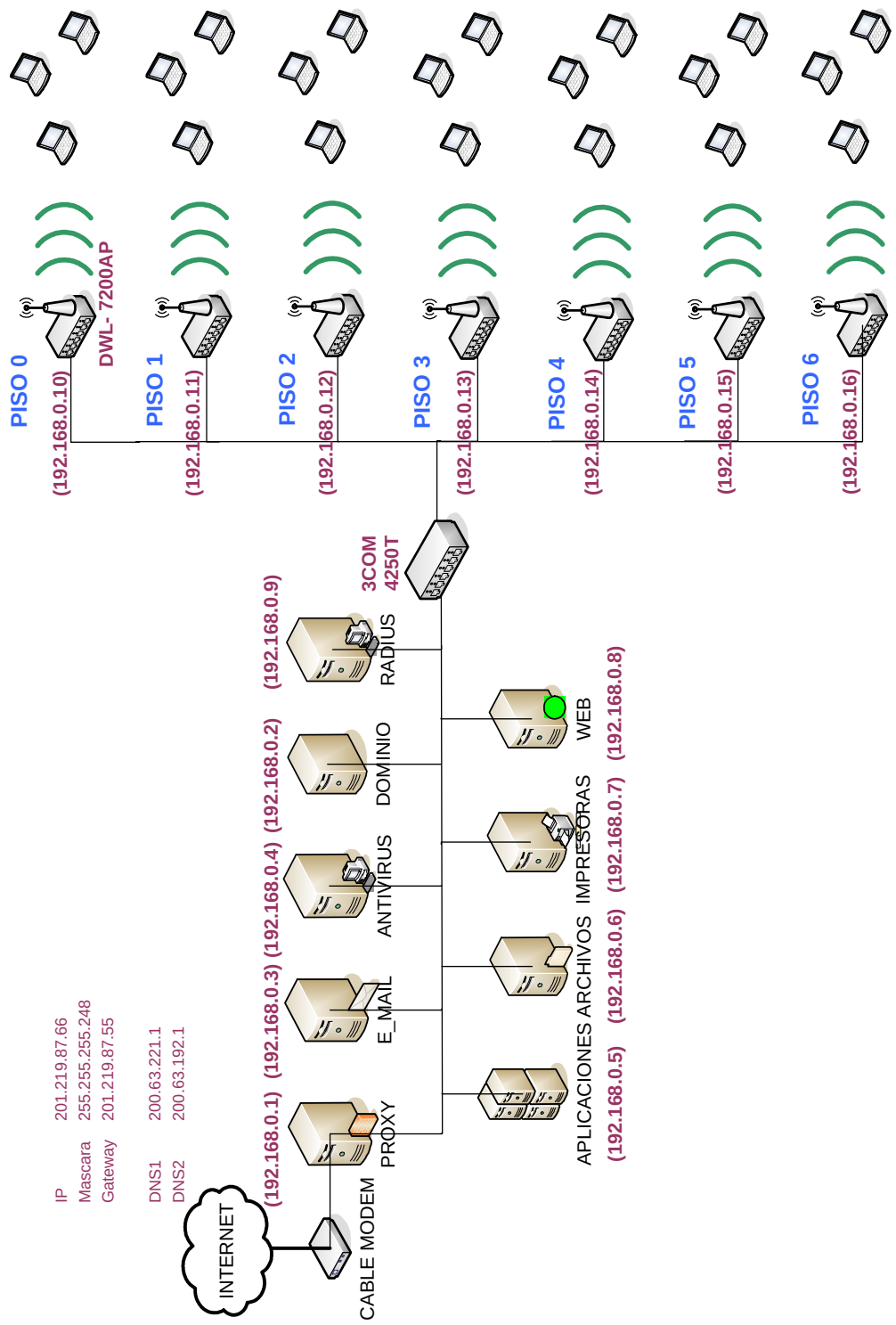


Figura 3.71. Diseño de red inalámbrica.

CAPÍTULO IV

SISTEMA DE SEGURIDAD CON CÁMARAS INALÁMBRICAS

En esta parte del proyecto se tratará un método de seguridad que es muy común en los edificios empresariales. Este método es un sistema de seguridad mediante cámaras IP inalámbricas con monitoreo remoto mediante Internet.

De forma inicial, el proyecto trata de cubrir con cámaras de seguridad toda el área de trabajo del edificio con la idea de tener un respaldo en video de todo el movimiento que se realiza diariamente en la empresa.

Para ingresar al edificio hay que registrar el nombre de la persona que ingresa en un libro que tiene la empresa, eso no representa una seguridad aceptable de ingreso. Con el sistema de monitoreo de cámaras de video esta seguridad mejorará considerablemente por lo que la empresa ha solicitado que se haga el estudio y diseño para instalar las mismas.

4.1 CRITERIOS DE DISEÑO

Para realizar un diseño de cámaras de seguridad existen algunos criterios que se deben tratar. A continuación se enlistan los principales parámetros que se deben tomar en cuenta para el diseño.

- Cobertura de la mayor área en cada piso.
- Amplio campo de visión (grados).
- Formato de compresión de video y audio.
- Fácil instalación
- Monitoreo simultáneo de varias cámaras.

- Nitidez de imagen a larga distancia
- Capacidad de captación de movimiento.

Todos estos parámetros deben ser analizados al momento de seleccionar los equipos que van a ser instalados.

4.2 SELECCIÓN DE CÁMARAS INALÁMBRICAS

Para tener una breve idea de la clase de equipos que se encuentran en el mercado se han seleccionada tres tipos de cámaras IP inalámbricas para hacer una comparación de sus características básicas como son: tipo de sensor, lente, iluminación, formato de audio y video, campo de visión, etc. y así poder escoger la mejor opción para el desarrollo del sistema de seguridad.

La siguiente tabla muestra la comparación de características entre las marcas Linksys-Cisco, D-Link y Sony.

	Linksys-Cisco	**Sony**	**D-Link**
Modelo	WVC200	SNC-M3	DCS-2120
Descripción	Cámara IP wireless 54 Mbps.	Cámara wireless IP Móvil	Wireless Internet SECURICAM
Estándares	802.11b y g.	802.11b y g.	802.11b y g.
Velocidad TX.	54 Mbps.	54 Mbps.	54 Mbps.

Sensor	1/5” CMOS (VGA)	1/4” CMOS (VGA)	1/4” CMOS (VGA)
Lente	3 mm.	3.7 mm.	4 mm.
Iluminación	2 Lux.	1.5 Lux.	0.5 Lux.
Compresión de video	MPEG MPEG - 4	MPEG - 4	MPEG - 4
Audio	Sin audio	16, 24, 32, 40 Kbps (AAC)	16~128kbps (AAC) 4.7~130kbps (GSM-AMR)
Campo de visión	61.48 grados	51 grados	62 grados
Monitoreo (# cámaras)	8	4	16
Movimiento de cámara	No	PAN/TILT	No
Seguridad Inalámbrica	WEP - WPA	WEP - WPA,	WEP - WPA
Precio Aproximado	$ 275	$ 385	$ 260

Tabla 4.1. Tabla comparativa de equipos.

Se han seleccionado las cámaras inalámbricas DCS-2120 de la marca D-Link para realizar este estudio por presentar características avanzadas y mejoradas con relación a las versiones anteriores de los equipos de la misma marca. Estas características se presentarán a continuación junto con una descripción detallada del equipo.

4.3 CAMARA INALÁMBRICA DCS-2120

La cámara de seguridad DCS-2120 es un poderoso sistema de vigilancia que se conecta a una red 802.11g. Esta cámara funciona bajo los estándares 802.11b y g y se conecta a una velocidad máxima de 54 Mbps. El DCS-2120

difiere de las cámaras convencionales por que posee un sistema CPU incluido y un servidor Web, es decir, se puede asignar a la cámara una dirección como por ejemplo www.seguridademopq.com y así los usuarios podrán acceder remotamente a la cámara sin tener que recordar la dirección IP, incluso si su proveedor de servicios Internet la ha cambiado. Este equipo permite tomar fotos instantáneas (Snapshot) y guardarlas directamente desde el navegador Web a un disco duro local sin necesidad de utilizar otro software.

La DCS-2120 ofrece una resolución de 640 x 480 a 30 cuadros por segundos, un zoom de 4x, además las imágenes o vídeos generados por el dispositivo son 3GPP7ISMA, por lo que pueden ser reproducidas en equipos de cómputo o celulares compatibles.

El software incluido permite al usuario ver hasta 16 cámaras en una única pantalla de ordenador y desde una única localización central. Las imágenes se pueden grabar manualmente o según una programación preestablecida. Los usuarios pueden configurar avisos automatizados de mensajes de correo electrónico que se envían por Internet para informar al instante de cualquier suceso inesperado

Con 0.5 lux de sensibilidad de luz (Unidad derivada del SI de iluminancia), la cámara es capaz de capturar video en habitaciones con un mínimo de iluminación. Tiene también capacidad de 4X de zoom. El DCS-2120 brinda la capacidad de monitorear video y audio en una estación de trabajo usando un explorador Web desde cualquier parte del mundo.

4.3.1 Requisitos de sistema

Los requisitos básicos para el funcionamiento de una cámara de seguridad DCS-2120 son:

- Windows® 2000 o XP
- 128 MB de memoria como mínimo (recomendado 256 MB)

- Red inalámbrica (802.11b o 802.11g) o Ethernet
- Navegador Web Internet Explorer 6.x
- Tarjeta VGA con resolución: 800 x 600 o superior
- CPU: procesador Pentium 4 a 1,3 GHz o superior (procesador Pentium 4 a 2.4 GHz o superior con 512 MB de memoria y un tarjeta de vídeo de 32 MB para la visualización y grabación de varias cámaras IP).

4.3.2 Características

- Grabación a baja iluminación gracias a sus 0.5 lux para grabar en la noche.
- Zoom digital 4X para una captación más cercana, lente de 4mm., 62 grados de campo de vista, sensor ¼" CMOS.
- Resoluciones de video a 160 x 120, 176 x 144, 320 x 240 y 640 x 480 pixeles a 30 fps (tomas por segundo).
- Configuración remota vía Internet o teléfonos celulares 3G.
- Son permitidos 20 nombres de usuarios y contraseñas con privilegios de configuración y control para administradores.
- Soporta una variedad de plataformas como son: TCP/IP, SMTP email, HTTP y otros protocolos de Internet.
- Pueden tomarse imágenes instantáneas de forma remota directamente del explorador Web a un disco duro local.
- Vigilancia avanzada y monitoreo local gracias a su software de vigilancia IP que permite administrar y modificar hasta 16 cámaras vía Intranet.
- Compatibilidad con clientes de teléfonos celulares 3G para mirar video en vivo por medio de una red celular con este servicio habilitado.
- Seguridad inalámbrica 64/128-bit WEP y WPA-PSK.
- Formato MPEG para foto sencilla y compresión de video mejorada usando MPEG4 bajo perfil simple.

4.3.3 Revisión de Hardware

La cámara de seguridad DCS-2120 tiene las siguientes medidas:

- Largo: 11.4 cm.

- Ancho: 7.9 cm.
- Profundidad: 4.1 cm.
- Peso: 185 g.

Parte frontal

Figura 4.1. Panel frontal de la cámara D-Link DCS-2120.

1. Antena: Antena para proporcionar conexión inalámbrica con una ganancia de 2dBi**.**

2. LED: En cuanto el adaptador de alimentación esté conectado a la cámara, el LED de alimentación empezará a parpadear en rojo y azul varias veces para indicar que la DCS-2120 está realizando un test. Terminado el test, el LED se iluminará de color azul para indicar que la conexión con el puerto Ethernet es correcta, o en rojo para indicar que tal conexión no se ha realizado.

Parte Lateral

Figura 4.2. Panel lateral de la cámara D-Link DCS-2120.

1. **Alimentación DC:** El conector de entrada de alimentación DC está etiquetado como DC 5V con un único jack de suministro de alimentación.
2. **Conector Ethernet:** La DCS-2120 dispone de un conector RJ-45 para conectarlo a una red cableada.

Parte Posterior

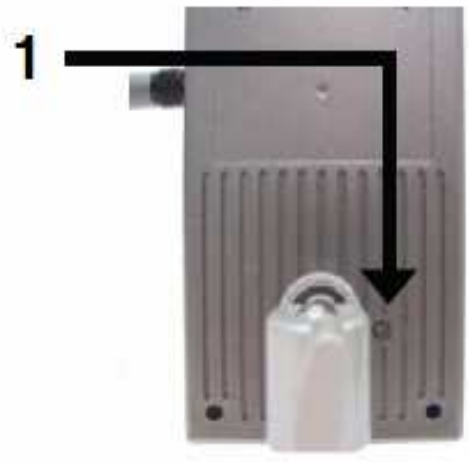


Figura 4.3. Panel posterior de la cámara D-Link DCS-2120.

1. **Botón Reset:** Al apretar el botón Reset una vez, el dispositivo se reinicia y el LED de alimentación empieza a parpadear.

Si se aprieta el botón Reset ininterrumpidamente durante 30 segundos, el dispositivo se reinicia con los valores por defecto.

4.4 DISEÑO DEL SISTEMA DE SEGURIDAD

El diseño del sistema de seguridad no consiste en otra cosa que cubrir, con los rangos de cobertura que brinda una cámara de seguridad, el área física que se quiere proteger tratando de obtener la mínima cantidad de espacios muertos (o sin cobertura) y también evitando que las áreas que cubren las cámaras sean interferidas entre si.

Estas coberturas se las realizan con más exactitud de forma manual, es decir, tratando de enfocar la mayor área moviendo la cámara de un lugar a otro hasta localizar el punto de mayor cobertura.

Para este diseño se realizarán coberturas teóricas tomando en cuenta las características del lente que posee la cámara. Para ello, se ha conseguido una tabla en la que se indica las distancias aproximadas a las que alcanza a enfocar cada lente la cual se muestra a continuación.

LENTE (mm.)	Alcance Horizontal (m.)	Alcance Vertical (m.)
2.8	17	12.9
4	14	9
6	8	6
8	6	4.5
12	4	3
16	3	2.3

Tabla 4.2. Alcance de lentes para cámaras.

El equipo tiene un lente de 4mm. Por lo que su alcance es de 14 metros en forma horizontal y 9 metros en forma vertical. Sabemos que cada piso del edificio tiene una distancia de 29.9 metros y una altura de 2.45 metros por lo que a simple vista se necesitaría dos cámaras por piso, en la cobertura vertical no hay ningún inconveniente ya que únicamente se debe cubrir 2,45 m. y la cámara abarca hasta 9 m. También tiene un campo de visión de 62 grados.

El siguiente gráfico indica el área de cobertura de cada cámara según las características de su lente, este gráfico esta hecho a la misma escala de los planos del edificio por lo que será utilizado para realizar la cobertura real.

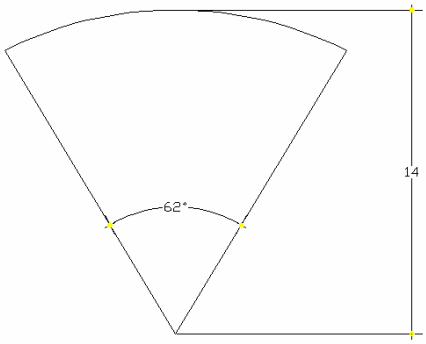


Figura 4.4. Área de cobertura de la cámara.

A continuación se realizará la cobertura teórica en los planos del edificio tratando de cubrir el total del área de trabajo.

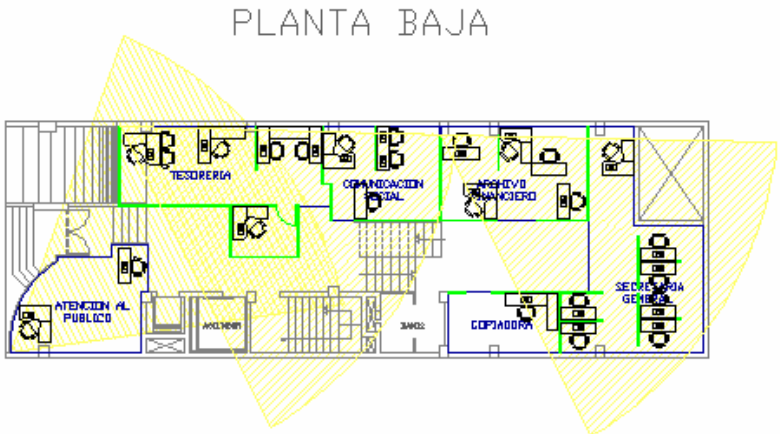


Figura 4.5. Cobertura planta baja.

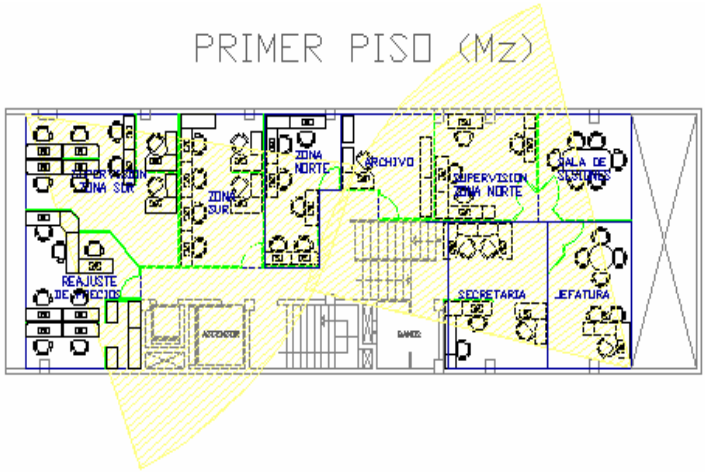


Figura 4.6. Cobertura primer piso.

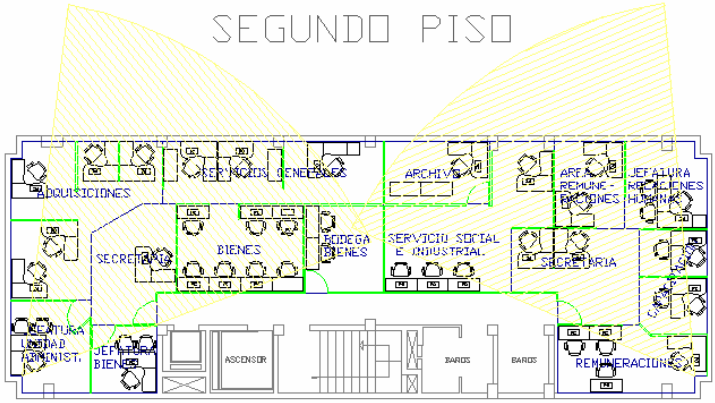


Figura 4.7. Cobertura segundo piso.

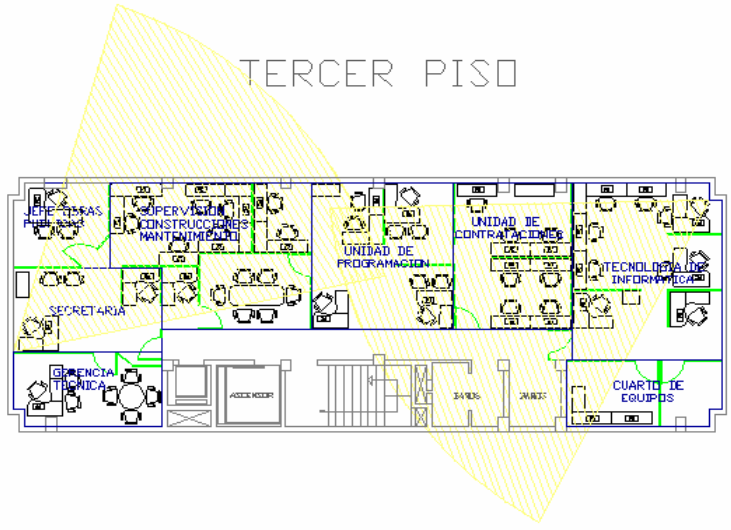


Figura 4.8. Cobertura tercer piso.

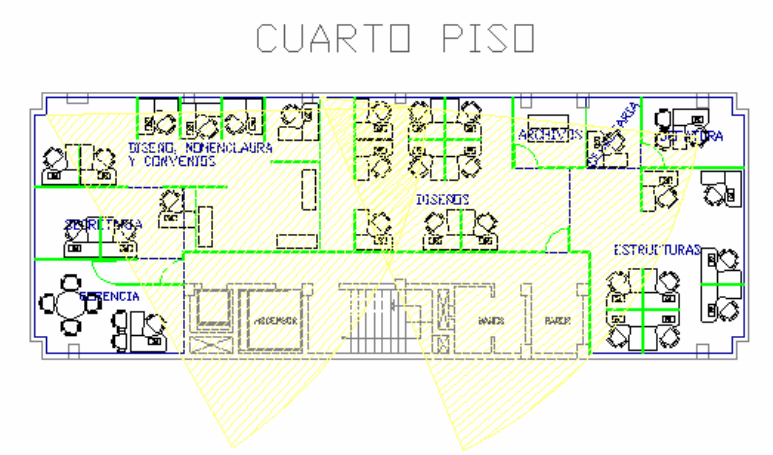


Figura 4.9. Cobertura cuarto piso.

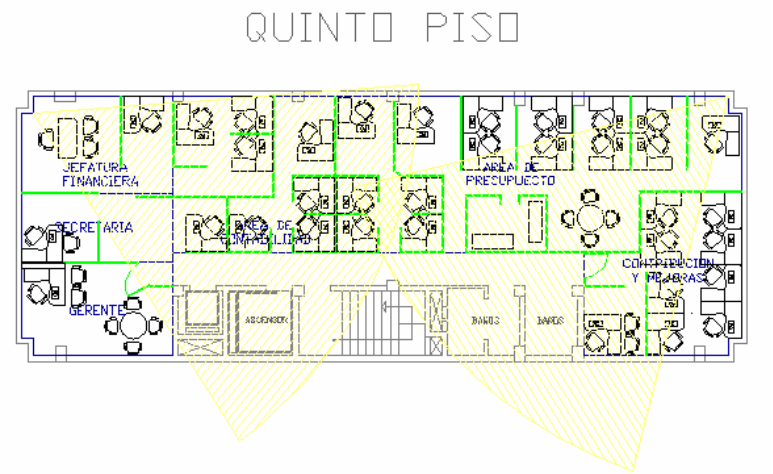


Figura 4.10. Cobertura quinto piso.

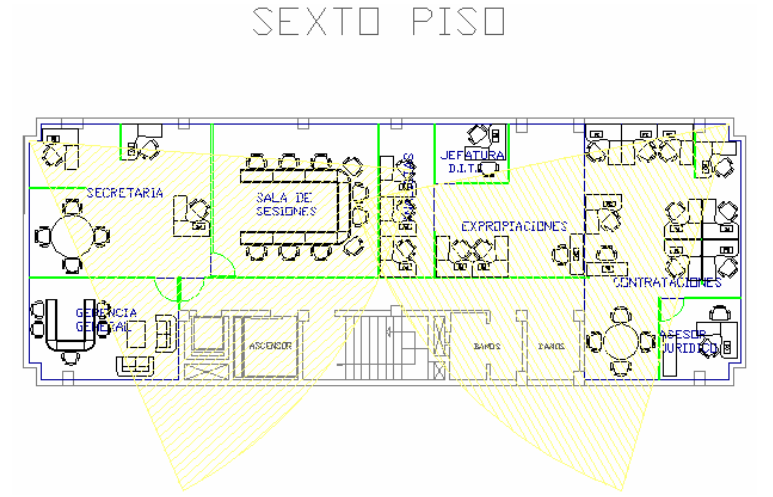


Figura 4.11. Cobertura sexto piso.

4.5 CONFIGURACIÓN DEL EQUIPO

Para configurar el equipo se debe instalar el asistente de configuración (Installation wizard) que se incluye en el CD de instalación. Al momento de arrancar el CD, aparece pantalla principal WIRELESS INTERNET CAMERA WITH 3G VIDEO SUPORT. Se selecciona Installation Wizard para instalar el asistente.

Figura 4.12. Instalación del software para configuración.

El asistente es una fácil interfaz para el usuario ya que le permite cambiar los parámetros generales relacionados con la cámara inalámbrica para que entre en funcionamiento de una manera rápida. Al iniciar el asistente aparece la pantalla principal que se muestra en la siguiente figura.

Figura 4.13. Network Camera installation.

En esta pantalla aparecerá el asistente de instalación, que mostrará la dirección MAC y la dirección IP de la cámara DCS-2120. Si se dispone de un servidor DHCP en la red, se mostrará una dirección IP válida, señalada con un “Yes” bajo la columna correspondiente.

Se pueden observar 5 pestañas que son: Setup, Upgrade, Reset to default, about y exit. La opción setup continúa la configuración de la cámara como se mostrará más adelante.

La opción Upgrade actualiza el firware del equipo. Si el firmware que tiene actualmente la cámara es más antiguo que el que está disponible para descargar, aparecerá un mensaje sugiriendo la actualización del mismo. Junto con este mensaje, la pantalla presenta la información acerca del firmware actual de la cámara.

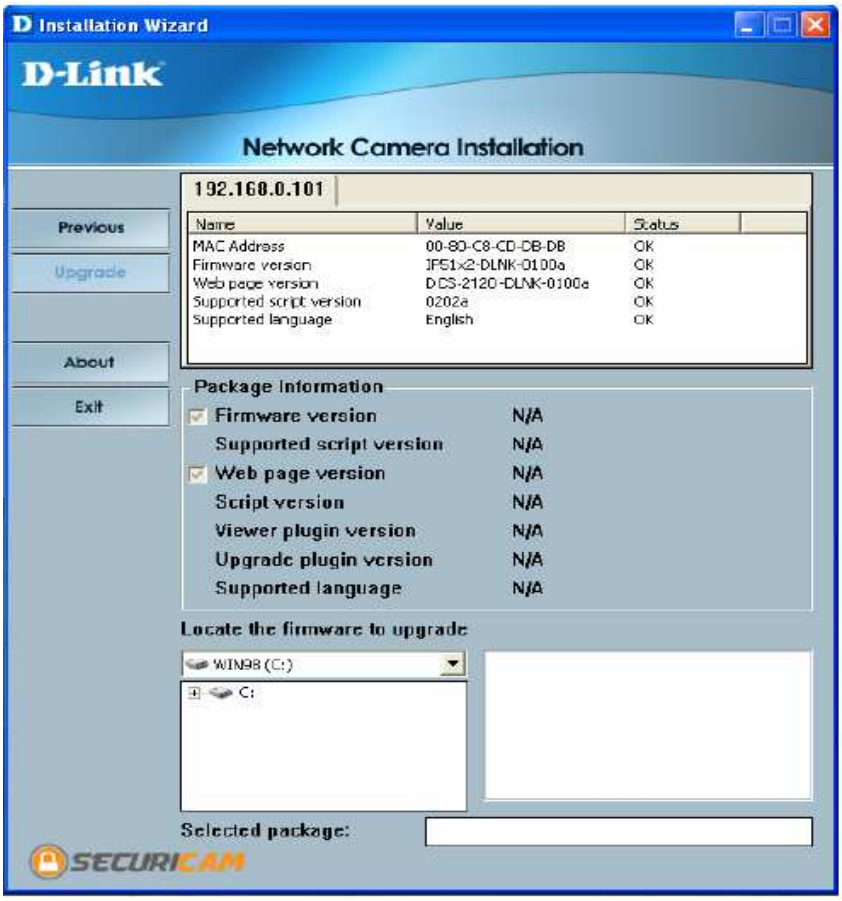


Figura 4.14. Información de firmware.

Figura 4.15. Mensaje de actualización de firmware.

La opción “reset to default” como su nombre lo indica, reinicia el equipo a la configuración de fábrica, es como hacer un reset al equipo mediante software. La opción “about” indica en una ventana la versión del software y la opción “exit” cierra el programa.

Si el asistente de instalación no detecta ningún dispositivo, se debe reiniciar la cámara. La cámara se reiniciará al apretar una vez el botón Reset y el LED de alimentación empiece a parpadear. Si se aprieta el botón Reset ininterrumpidamente durante 30 segundos, se reiniciará con los valores por defecto. Luego de reiniciar el equipo se oprime el botón “Search” para buscar nuevamente las cámaras conectadas como se indica en la siguiente figura.

Figura 4.16. Buscando cámaras.

Una vez que se el software ha encontrado la cámara, se presiona el botón “Setup” para empezar a configurarla con los parámetros que aparecen en cada pantalla.

Al entrar al Setup encontramos 5 pestañas que son: previous, next, skip, about y exit. Junto a estas pestañas aparece una pantalla de configuración en la que se ingresan los siguientes datos:

- Un nombre a la cámara.
- Una contraseña y la confirmación de la contraseña.
- Configuración de hora y fecha, la cual puede ser configurada con la misma fecha y hora del computador donde está instalado el software también y se puede ingresar esta información de modo manual.

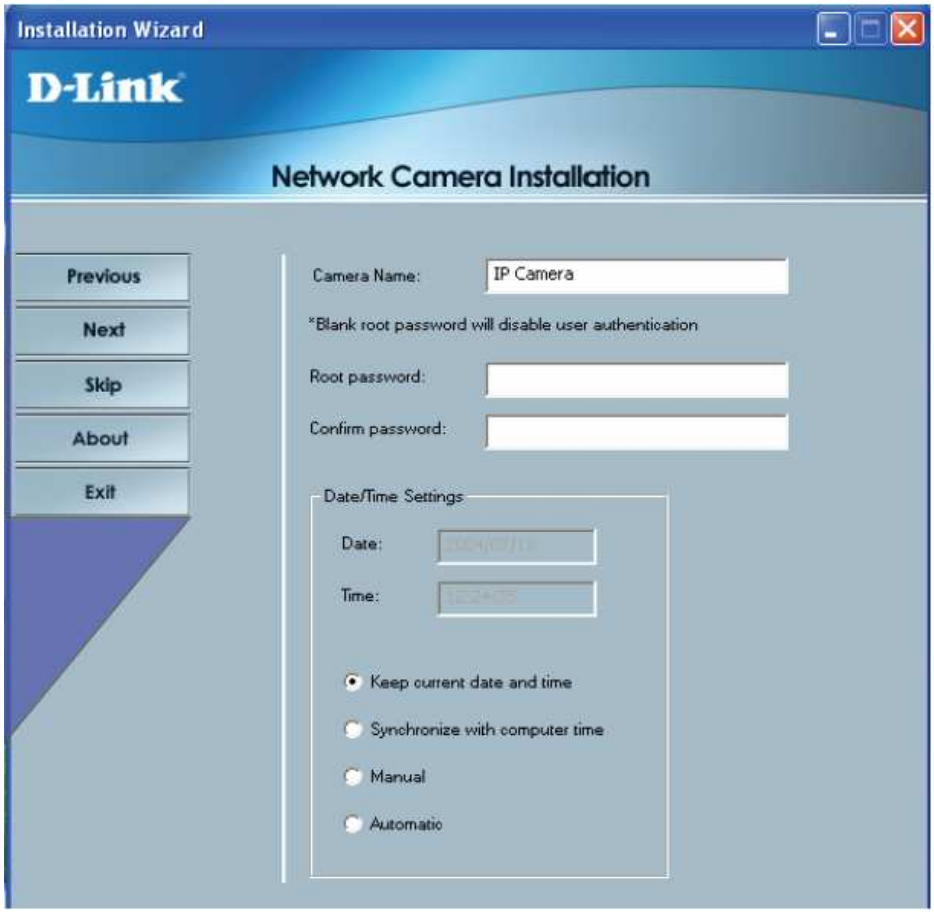


Figura 4.17. Configuración de cámaras.

En “next” se ingresa a otra pantalla para las configuraciones de red de la cámara como la dirección IP, la mascara de subred, default router (opcional), DNS primario y secundario. Para mantener la dirección IP asignada se debe desmarcar la opción “Reset IP address at next boot. A continuación se muestra la ventana.

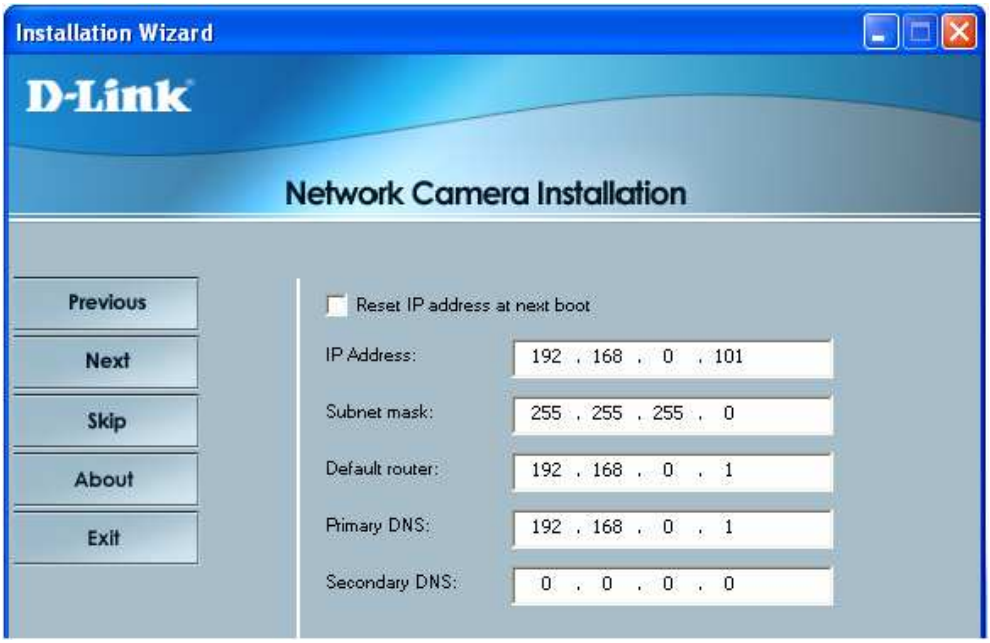


Figura 4.18. Configuración de red.

Nuevamente al pulsar en “next” pasamos a la siguiente ventada de configuración de red en la cual se ingresan parámetros como el SSID de la red, el modo de red inalámbrica (en este caso infraestructura), el canal de funcionamiento, la velocidad de transmisión y el modo de preámbulo. También se ingresa la encriptación de datos que va a ser WPA igual que los access points tratados en el capítulo anterior.

(SIGUIENTE HOJA)

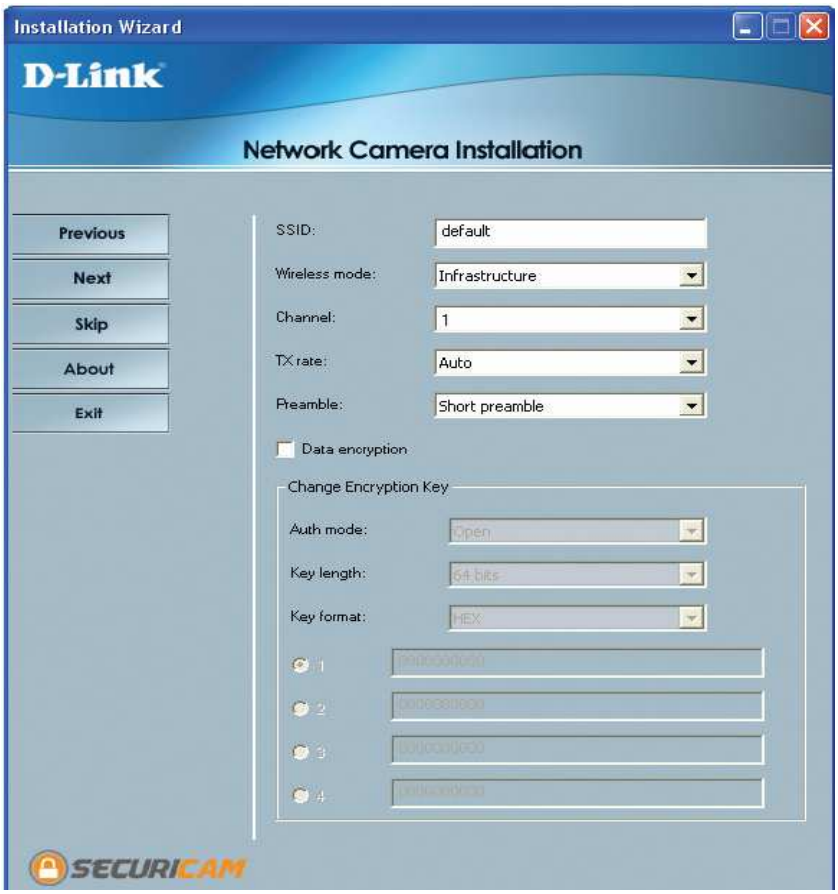


Figura 4.19. Configuración de red (continuación).

Finalmente se presiona otra vez el botón next para pasar a la última ventana en la que se permite guardar todas las configuraciones realizadas a la cámara. La última ventana presenta una opción “Apply” que al presionar ese botón se guardarán las configuraciones.

Para poder ver la cámara en el explorador Web después de haberla configurado, se puede ingresar yendo a mis sitios de red en el escritorio de Windows. Ahí se encuentra un icono con la dirección IP de la cámara de la siguiente manera.

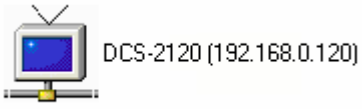


Figura 4.20. Icono del explorador para la cámara IP.

También se puede ingresar por medio del explorador Web ingresando la dirección IP de la cámara, de manera similar como se hace para ingresar a los access points.

Esta configuración que se ha explicado permite que las cámaras funcionen sin ninguna configuración especial. Las configuraciones avanzadas se las realiza por medio del menú de la cámara que aparece al ingresar la dirección IP de la misma en un browser.

4.6 SOFTWARE PARA SISTEMA DE VIGILANCIA

El software de vigilancia IP que viene incluido en el CD de instalación de las cámaras convierte a los DCS-2120 en un poderoso y flexible sistema de vigilancia para empresas y hogares. Las características del software son las siguientes:

- Monitoreo en tiempo real.
- Grabación de video en disco duro.
- Video de alta calidad.
- Alta compresión de video.
- Máximo 16 cámaras con diferentes diseños de visualización.
- Reproducción elegante.
- Búsqueda rápida en base de datos.
- Alarmas configurables.
- Protección con cuenta de contraseña.
- Programación de grabación para cada cámara.
- Fotos instantáneas vía Email/FTP.
- Detector de movimiento en cada cámara.

Para instalar el programa de vigilancia se hace clic en “IP surveillance” que se encuentra en la misma pantalla inicial que aparece al ejecutar el CD de instalación.

Figura 4.21. Instalación del sistema de vigilancia.

La única consideración que debe hacerse en la instalación del software es al momento que se pide que se ingrese una contraseña para el administrador. Esta contraseña es la que permitirá ingresar al programa de vigilancia por medio del usuario “admin”, de no recordar esa contraseña es imposible ingresar al programa y tocaría instalarlo de nuevo.

Esta es la parte en que la instalación pide un password y una confirmación del password ingresado.

Figura 4.22. Password del usuario admin.

4.6.1 Ventana de monitoreo

Esta sección muestra una vista global del programa de monitoreo. Hay 8 grupos de funciones en la pantalla de monitoreo que serán explicadas con detalle más adelante. Estas funciones son:

- Misc. Funtions.
- Channel Area.
- Layout Area.
- Hard disck Status.
- Common Control Area.
- DI/DO Control.
- Alert message.
- Video Area.

Al momento de arrancar el programa se pide ingresar la contraseña de administrador con la que fue instalado. Tanto como el usuario como la contraseña pueden ser cambiadas según lo requiera el administrador de red. La pantalla que se presenta es la siguiente.

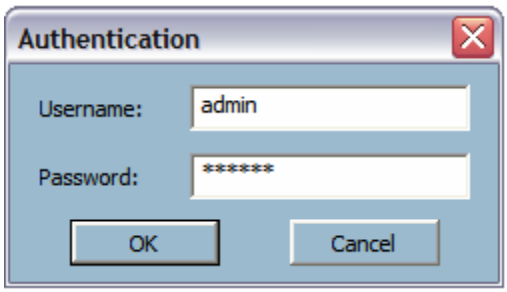


Figura 4.23. Pantalla principal de monitoreo.

Las funciones del monitor serán introducidas con detalle en las secciones siguientes. La pantalla principal de monitoreo se presenta en el gráfico siguiente.

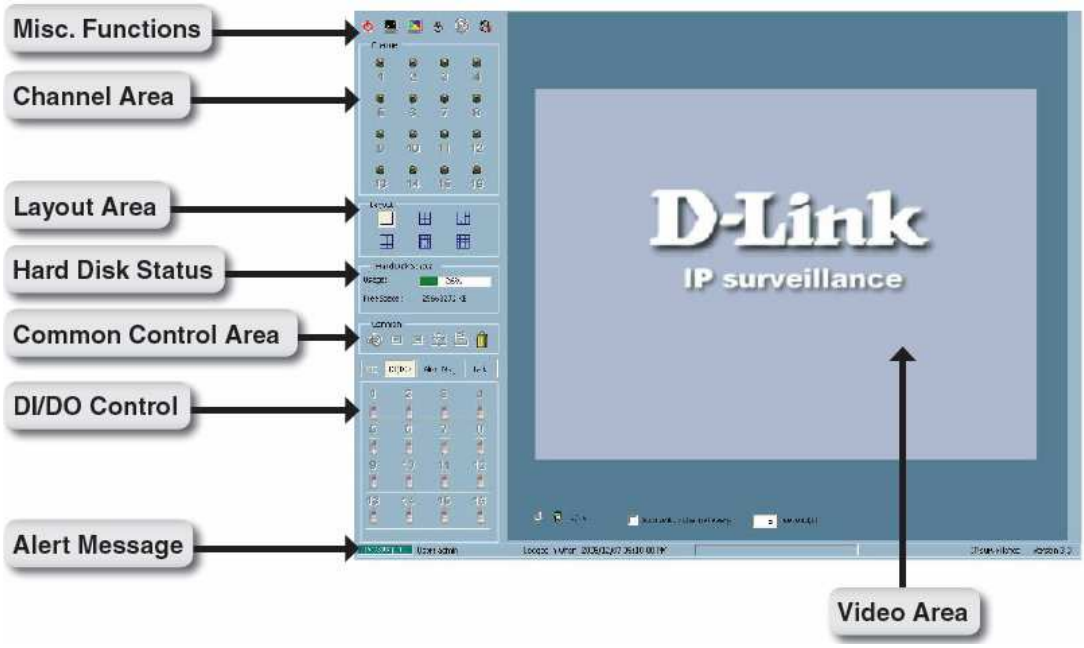


Figura 4.24. Pantalla principal de monitoreo.

Misc. Functions: En esta parte se incluye la aplicación de exit (salida del monitor), minimización de la ventana, monitoreo en pantalla completa, bloqueo, detener alerta y un menú de configuración para la cámara, configuraciones globales, configuraciones de calendario y la información del usuario en esta aplicación.

Figura 4.25. Misc. Functions.

Channel area: Esta área muestra el estado de cada canal de video. La información indica el estado de conexión, grabación, y selección. Cada una de las pantallas de cada cámara instalada se le puede agregar a cada uno de los canales de esta sección para poder organizar las imágenes según la conveniencia de la empresa.

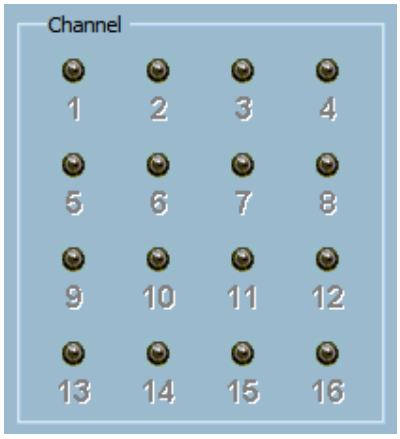


Figura 4.26. Channel area.

Video area: En esta área, se puede observar el video de un canal seleccionado en el marco de visualización (display frame). El número de marcos de visualización en el área de video depende del diseño que se haya escogido en el área de diseño (layout area).

Layout area: Se puede cambiar el diseño de monitoreo en esta área. Hay 6 tipos de diseños: 1, 4, 6, 9, 13 o 16 ventanas de visualización de video en el área de video.

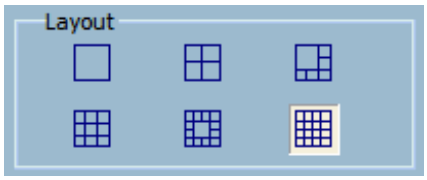


Figura 4.27. Layout area.

El gráfico anterior indica que se ha seleccionado el modo 16 ventanas, a manera de ejemplo se indica a continuación la ventana que aparece al seleccionar este modo.

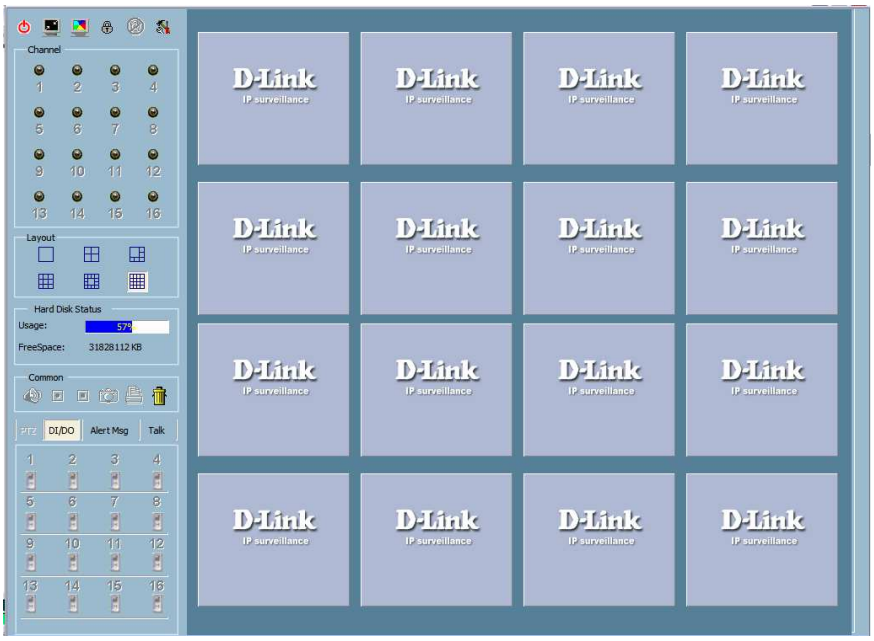


Figura 4.28. Área de 16 cámaras.

Hard disk status: En esta área se puede obtener el estado del disco duro de la base de datos de video residentes. Se puede observar el espacio que se ha utilizado con los videos que ya han sido grabados y también se puede ver la cantidad de espacio sobrante para grabar.

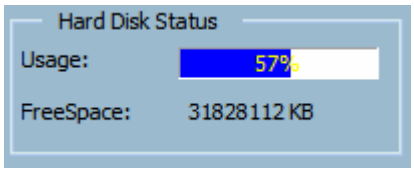


Figura 4.29. Hard disck status.

Common control area: Esta área incluye el control de volumen, grabación manual, impresión de video, fotos instantáneas y el “basurero” para remover videos desde las ventanas de visualización.

Figura 4.30. Hard disck status.

DI/DO control: Esta herramienta recibe la señal digital de entrada y envía una señal digital de salida al servidor de video remoto asociada con los canales de video dedicado.

Figura 4.31. DI/DO control.

Alert Message: Esta herramienta mostrará los últimos mensajes recibidos por el servidor de video remoto asociado con los canales de video seleccionados.

Figura 4.32. Alert message.

4.7 CONFIGURACIONES AVANZADAS

Las configuraciones avanzadas se las va a realizar por medio del explorador Web, ingresando la dirección IP de la cámara con lo que aparece la pantalla principal que se muestra a continuación en la que seleccionamos “Configuration”.

(SIGUIENTE HOJA)

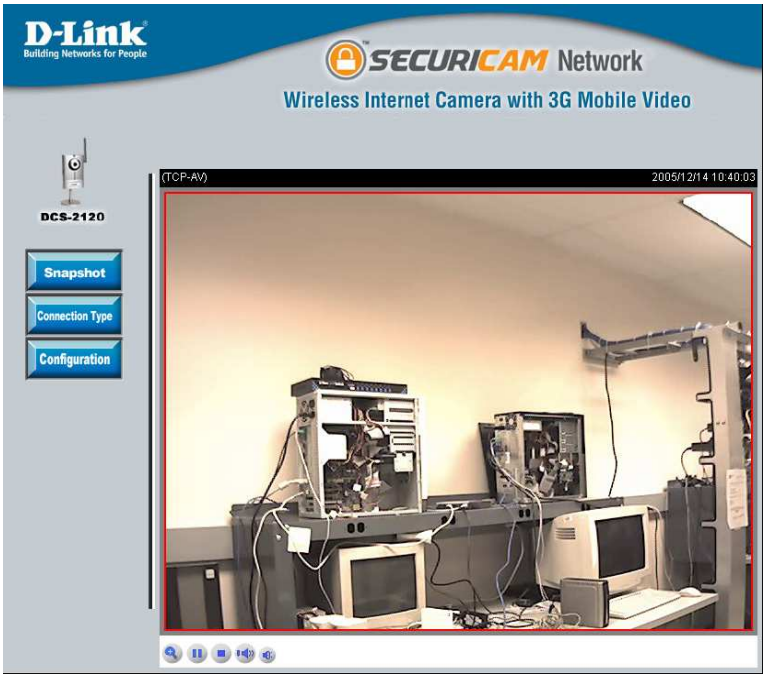


Figura 4.33. Pantalla de Inicio de la cámara.

Al entrar en “Configuration” encontramos 5 pestañas que son: inicio, avanzados, herramientas, estado y ayuda. Hay varias opciones de configuración pero únicamente vamos a indicar las configuraciones primordiales que son, por ejemplo, configuración de audio y video, configuración de imagen y la habilitación de la detección de movimiento.

Configurando estos parámetros obtenemos un mejor desenvolvimiento del software de vigilancia IP que se indicó anteriormente.

En la pestaña “avanzados” encontramos los botones “Audio/Video”, “Image Settings” y “Motion detection”.

4.7.1 Audio/Video

General. Permite configurar el modo del video, es decir, si se accederá remotamente a las cámaras por medio de un computador o un teléfono móvil.

Video Settings. Permite configurar la resolución del video, la frecuencia de línea, la tasa máxima de los frames, la calidad del video y la orientación de video (volteado o espejo).

Audio Settings. Permite seleccionar el formato del audio y la tasa de bits de audio.

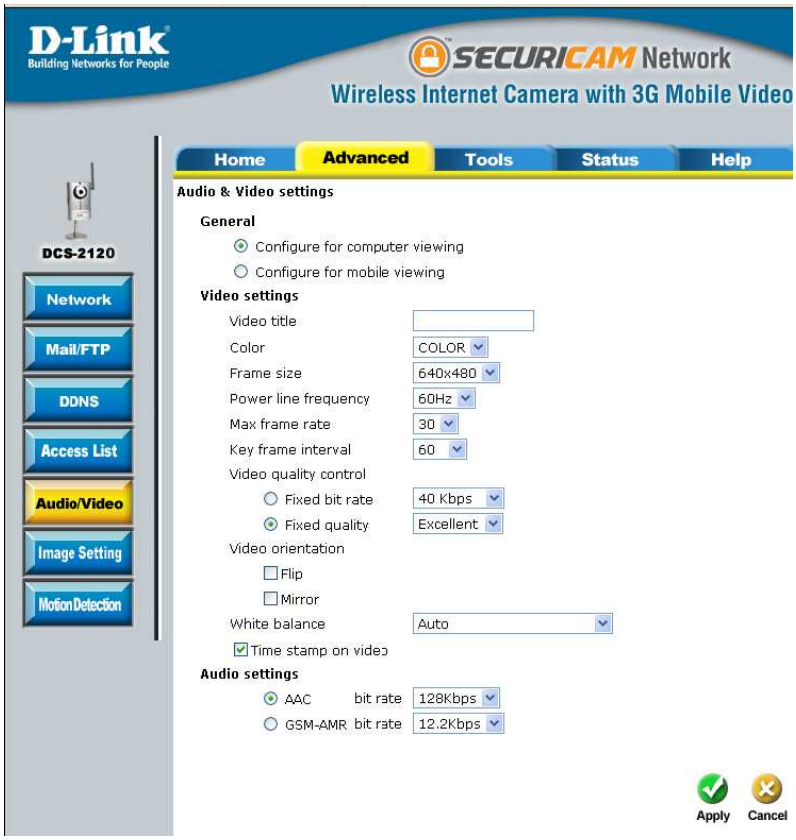


Figura 4.34. Audio/Video.

4.7.2 Image Settings

Se configura el brillo, la nitidez, el contraste y la saturación de cada una de las cámaras.

(SIGUIENTE HOJA)

Figura 4.35. Image Settings.

4.7.3 Motion Detection

Enable motion detection. Habilita el modo de detección de movimiento.

Window name. Es el nombre de la ventada de detección de movimiento.

Sensitivity. Ajusta la sensibilidad de detección al movimiento. Si la sensibilidad esta en el nivel más alto el mínimo movimiento será detectado por las cámaras.

Percentage. Ajusta los porcentajes que permite que se “setee” un requisito cuánto la ventana de movimiento deber ser llenada por la imagen en del movimiento, por ejemplo, si se pusiera este a 50 %, entonces la ventana seleccionada debe ser llenada por un objeto en movimiento antes de que provoque la detección otro movimiento.

New. Agrega ventanas de monitoreo de un área específica. Se puede ingresar hasta 3 ventanas de detección de movimiento.

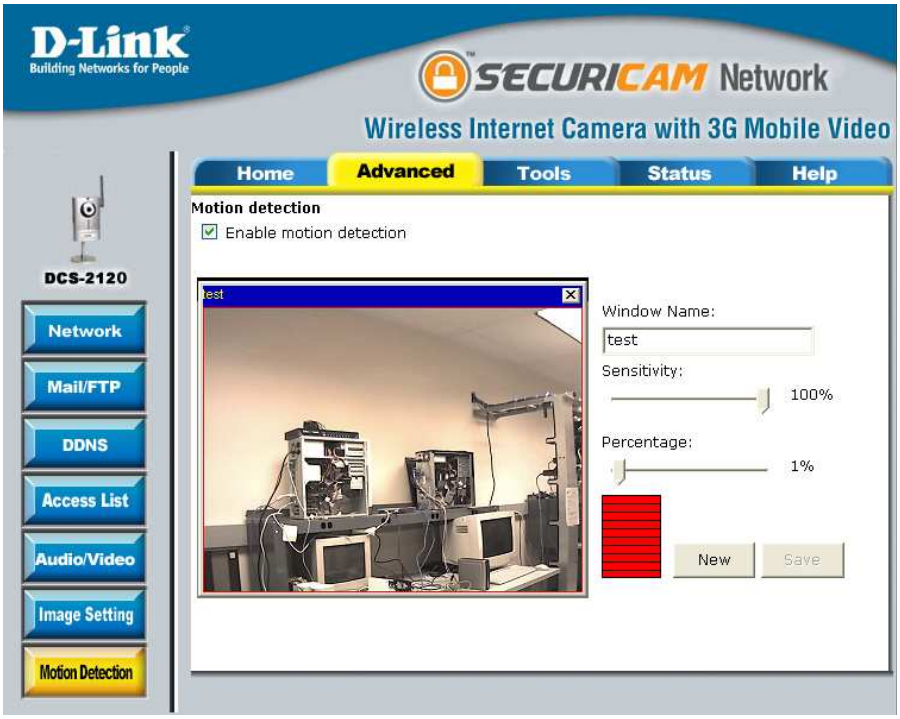


Figura 4.36. Motion detection.

4.8 RESUMEN DE CONFIGURACIONES

A continuación se presenta un resumen de las configuraciones realizadas para la instalación de las cámaras inalámbricas y también para el software de monitoreo.

CAMARA IP	CANAL	DIRECCIÓN IP	MASCARA DE SUBRED	PUERTO
Piso 0	1	192.168.0.101 192.168.0.102 192.168.0.103	255.255.255.0	80 81 82
Piso 1	4	192.168.0.104 192.168.0.105	255.255.255.0	83 84
Piso 2	7	192.168.0.106 192.168.0.107	255.255.255.0	85 86
Piso 3	11	192.168.0.108 192.168.0.109	255.255.255.0	87 88
Piso 4	1	192.168.0.110	255.255.255.0	89

		192.168.0.111		90
Piso 5	4	192.168.0.112 192.168.0.113	255.255.255.0	91 92
Piso 6	7	192.168.0.114 192.168.0.115	255.255.255.0	91 92

Tabla 4.3. Resumen de configuraciones

Para realizar la configuración de monitoreo remoto se debe adquirir una dirección IP pública del proveedor de ISP, ya que el equipo tiene un servidor web incorporado y para acceder a el remotamente debe tener una dirección q electrónica que va a ser www.seguridademopq.com. Esta configuración se la realiza de la misma forma que cuando se ingresa una dirección IP para la cámara inalámbrica.

CAPÍTULO V

ANÁLISIS DE COSTOS

Este capítulo trata sobre los costos de equipos e implementación que tienen tanto el diseño de la red inalámbrica como el diseño del sistema de seguridad con cámaras inalámbricas. A continuación se muestran los detalles de cada proyecto.

5.1 ANÁLISIS DE COSTOS PARA LA RED INALÁMBRICA

5.1.1 Costos de equipos

Según el diseño realizado, para la red inalámbrica se necesitan los siguientes equipos:

- 7 ACCESS POINTS DWL-7200AP
- 210 ADAPTADORES USB INALÁMBRICOS DWL-AG132
- SERVIDOR RADIUS FREERADIUS
- SISTEMA OPERATIVO LINUX

El número de adaptadores inalámbricos puede variar según la cantidad de host que se encuentren habilitados al momento de hacer la instalación de los equipos (si ha existido cambios en la red), tomando en cuenta también el número de computadoras portátiles que disponga la empresa. Al momento de hacer el diseño se contabilizaron 210 host habilitados por lo que la cotización se realizará con 210 adaptadores USB.

En el siguiente cuadro se presenta los valores referenciales de los equipos.

No.	*DESCRIPCIÓN*	*V. UNITARIO*	*V. TOTAL*
7	Access Point D-link DWL-7200 AP (**)	$ 170	$ 1.190,00
210(*)	Adaptadores USB DWL- AG132 (**)	$ 48	$ 10.080,00
		Subtotal	$ 11.270,00
		+ 12% IVA	$ 1.352,40
		TOTAL	$ 12.622,40

(*) Cantidad sujeta a cambios, por actualizaciones o cambios internos

(**) Precios referenciales de la Empresa PC-WARE

Tabla 5.1. Cotización de equipos para la red inalámbrica.

5.1.2 Costo de implementación y configuración

La implementación y configuración se la realizará en un período de 10 días a partir de la entrega de los equipos.

No.	*DESCRIPCIÓN*	*V. TOTAL*
7	Instalación y configuración de Access Points D-link DWL-7200AP	$ 140,00
210 (*)	Instalación y configuración de adaptadores inalámbricos USB DWL-AG132	$ 2100,00
1	Instalación y configuración de servidor Radius	$ 50,00
	TOTAL	$ 2290,00

(*) Cantidad sujeta a cambios

Tabla 5.2. Cotización de instalación para el sistema de red inalámbrica.

5.2 ANÁLISIS DE COSTOS PARA EL SISTEMA DE SEGURIDAD

5.2.1 Costos de equipos

Para el diseño expuesto se necesitan los siguientes equipos:

- 15 CÁMARAS IP INALÁMBRICAS

En el siguiente cuadro se presenta la cotización que ofrece la empresa PC-WARE.

No.	***DESCRIPCIÓN***	***V. UNITARIO***	***V. TOTAL***
15	Cámaras D-link DCS-2120	$ 245	$ 3.675,00
		Subtotal	$ 3.675,00
		+ 12% IVA	$ 441,00
		TOTAL	$ 4.116,00

Tabla 5.3. Cotización de equipos para el sistema seguridad.

5.2.2 Costo de implementación y configuración

La implementación y configuración se la realizará en un período de 5 días a partir de la entrega de los equipos.

No.	***DESCRIPCIÓN***	***V. TOTAL***
15	Instalación de Cámaras D-link DCS-2120	$ 150,00
15	Configuración de cámaras	$ 50,00
1	Instalación y configuración de software de sistema de monitoreo	$ 50,00
	TOTAL	$ 250,00

Tabla 5.4. Cotización de instalación para el sistema de seguridad.

5.3 COSTO TOTAL DEL PROYECTO

El costo total del proyecto se resume en la tabla que se presenta a continuación.

DESCRIPCION	***VALOR***
Instalación y configuración de red inalámbrica	$ 14.912,40
Instalación y configuración de sistema de seguridad	$ 4.366,00
TOTAL	$ 19.278,40

Tabla 5.5. Cotización de instalación del proyecto completo.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Las redes inalámbricas tienen mucho auge en la actualidad y comúnmente son muy aplicadas en redes de hogar, pequeñas y medianas empresas. El estudio que se realizó para el edificio de la EMOP-Q es un estudio factible para su implementación considerando las características que presenta la red actual y los requerimientos de seguridad y movilidad.

- Para realizar la implementación wireless empresarial lo mejor es utilizar la infraestructura existente, es decir, el backbone de la red es de gran utilidad ya que se puede incluir los equipos inalámbricos necesarios para su actualización y mejoramiento y de esta manera obtener mejoras en velocidad de transmisión.

- Los mapas de cobertura son uno de los procedimientos más importantes en los diseños de redes inalámbricas. Un correcto desarrollo de estos mapas permiten que la red funcione de manera óptima.

- En la actualidad existe software que realiza el análisis espectral para dimensionar la “pisada” de la señal inalámbrica en el entorno físico con lo que se podría optimizar la correcta ubicación de los puntos de acceso, especialmente cuando se tienen casos críticos de cobertura. Este software poseen las empresas que se dedican al diseño de

redes inalámbricas y también se los puede adquirir por Internet a un precio elevado.

- La seguridad en redes inalámbricas de infraestructura es muy importante al momento de diseñar redes WI-FI. Para estos casos los servidores RADIUS son el método de seguridad más efectivo y más usado en el ámbito empresarial inalámbrico.

- Los sistemas de vigilancia con cámaras IP se han desarrollado de tal forma que en la actualidad se los puede implementar de una manera muy rápida y sencilla. Estos sistemas son de gran ayuda para la seguridad de una empresa en la que a diario circula mucha gente.

6.2 RECOMENDACIONES

- Antes de realizar un diseño de red inalámbrica es necesario hacer pruebas dentro y fuera del área donde se quiere instalar una red de este tipo con el fin de detectar si existen redes inalámbricas cercanas que podrían causar algún tipo de interferencia. Para efectuar estas pruebas, existen programas que envían señales WI-FI para detectar alguna respuesta y por lo tanto detectar una red inalámbrica, o realizar un barrido espectral con un analizador de espectros.

- Para las redes inalámbricas, aparte del desarrollo teórico que incluye el análisis de los equipos a utilizar, es necesario hacer mediciones de calidad y potencia de la señal. Esta es una tecnología que depende de factores externos como las interferencias y el clima. La parte teórica no es suficiente para obtener buenos resultados

- Se recomienda analizar la compatibilidad de los equipos que se van a seleccionar, con los adaptadores de las distintas marcas que existen en el mercado para obtener un alto rendimiento en la conexión.

- Es necesario realizar una revisión de los sectores que mas flujo de personas tenga, para ubicar de mejor manera las cámaras inalámbricas y cubrir mejor el área de influencia.

- Para los sistemas de seguridad es recomendable comunicarse con el proveedor de Internet y realizar el pedido de una dirección IP publica válida, para poder configurar el servicio de monitoreo remoto.

D-Link
Building Networks for People

DWL-7200AP

AirPremier AG

Wireless AG Access Point with PoE

FEATURES

Robust Network Options

- Adds 802.11a and 802.11g Dualband Connectivity to Existing Network
- Concurrently Provides Maximum Bandwidth of up to 108Mbps[1] in Both 802.11a and 802.11g
- 802.11g is Backward Compatible with 802.11b Networks and Devices
- Assign Users to 2.4GHz or 5GHz Frequency Bands

Multiple Operation Modes

- Access Point
- Point-to-Point (PtP) Bridge
- Point-to-Multipoint (PtMP) Bridge
- Repeater
- AP Client

Enhanced Security Features

- 802.1x
- WPA
- AES
- MAC Address Filtering
- Disable Broadcast SSID

Convenient Installation

- Supports 802.3af Power over Ethernet
- Detachable Antennas

Intuitive Management Platforms

- AP Manager
- Web Browser (HTTP or HTTPS
- Telnet
- D-View SNMP v.3

D-Link, the industry pioneer in wireless networking, introduces a performance breakthrough in wireless connectivity – the D-Link *Air*Premier® AG DWL-7200AP Wireless Access Point, a business-class access point designed for small to medium businesses looking to deploy dualband multimode networks capable of delivering high performance speeds in both the 802.11a and 802.11g bands – at the same time.

The DWL-7200AP is an ideal solution for creating a secure and robust dualband wireless network. With its capability to concurrently perform and support users in both 2.4GHz and 5GHz frequency without splitting up the bandwidth per band, the DWL-7200AP provides administrators with greater flexibility in network deployments. For advanced installations, this new high-speed Access Point has an integrated 802.3af Power over Ethernet (PoE) port that allows you to install the device in areas where power outlets are not readily available. The current default 5dBi high-gain antennas can also be replaced if a stronger wireless signal is needed.

The DWL-7200AP provides maximum wireless security by supporting both WPA-Personal and WPA-Enterprise which includes 802.1x user authentication. Other security features included in this Access Point are MAC Address Filtering, Wireless LAN segmentation, Disable SSID Broadcast, and support for Advanced Encryption Standard (AES) Encryption.

To maximize your return on investment, the DWL-7200AP can be configured in any one of five modes: Access Point (AP), Point-to-Point (PtP), Point-to-Multipoint (PtMP) bridge, Repeater, or AP Client. With the ability to simultaneously operate in two bands, network administrators can assign one mode in 802.11a and another in 802.11g to increase productivity and maintain high network efficiency.

Powered by D-Link 108AG technology, the DWL-7200AP delivers unparalleled wireless performance boasting maximum wireless signal rates of up to 108Mbps[1] when set in Turbo mode for both 802.11a and 802.11g networks. Meanwhile, wireless devices operating on the 802.11g band remain backward compatible to standard 802.11b devices. With the ability to deliver high-throughput transfer rates in two bands at the same time, the DWL-7200AP provides reliable bandwidth performance while providing a solution to avoid network bottlenecks.

Network administrators can manage all the DWL-7200AP's settings via its Web-based configuration utility or with Telnet. For advanced network management, D-Link's AP Manager or D-View SNMP management software offers an all-in-one method to configure multiple access points from a single location.

With dualband capabilities, integrated PoE support, extensive manageability, versatile operation modes and solid security enhancements, the new D-Link *Air*Premier AG Wireless Access Point with PoE provides everything needed to set up a future-proof wireless network or simply extend the wireless range of an existing network of today's small to medium businesses.

Product Data Sheet

AirPremier AG

DWL-7200AP

Wireless AG Access Point

Specifications

Standards
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.3
- IEEE 802.3af
- IEEE 802.3u
- IEEE 802.3x

Device Management
- Web-Based – Internet Explorer v6 or later; Netscape Navigator v7 or later; or other Java-enabled browsers.
- Telnet
- AP Manager
- SNMP v.3

Signal Rate[1]
For 802.11a/g:
- 108, 54, 48, 36, 24, 18, 12, 9 and 6Mbps

For 802.11b:
- 11, 5.5, 2, and1Mbps

Security
- 64-, 128-, 152-bit WEP
- WPA – Wi-Fi Protected Access (WPA – TKIP/AES PSK)
- 802.1x (EAP-MD5/TLS/TTLS/PEAP)
- MAC Address Access Control List

Wireless Frequency Range
- 2.4GHz to 2.4835GHz
- 5.15GHz to 5.35GHz and 5.725GHz to 5.825GHz

Radio and Modulation Type
For 802.11b:
DSSS:
- DBPSK @ 1Mbps
- DQPSK @ 2Mbps
- CCK @ 5.5 and 11Mbps

For 802.11a/g:
OFDM:
- BPSK @ 6 and 9Mbps
- QPSK @ 12 and 18Mbps
- 16QAM @ 24 and 36Mbps
- 64QAM @ 48, 54 and 108Mbps

DSSS:
- DBPSK @ 1Mbps
- DQPSK @ 2Mbps
- CCK @ 5.5 and 11Mbps

Wireless Operating Range[2]
802.11g (Full Power with 5dBi gain diversity dipole antenna)
Indoors:
- 98ft (30m) @ 54Mbps
- 105ft (32m) @ 48Mbps
- 121ft (37m) @ 36Mbps
- 148ft (45m) @ 24Mbps
- 203ft (62m) @ 18Mbps
- 223ft (68m) @ 12Mbps
- 253ft (77m) @ 9Mbps
- 302ft (92m) @ 6Mbps

Outdoors:
- 328ft (100m) @ 54Mbps
- 968ft (295m) @ 11Mbps
- 1378ft (420m) @ 6Mbps

Antenna Type
- Detachable Dipole antenna with 5dBi gain

Operating Voltage
- 48VDC +/- 10% for PoE

Transmit Output Power
For 802.11a:
- 63mW (18dBm)
- 40mW (16dBm)
- 32mW (15dBm)
- 6mW (7dBm)
- 1mW (0dBm)

For 802.11b:
- 63mW (18dBm)
- 40mW (16dBm)
- 32mW (15dBm)
- 23mW (13dBm)
- 10mW (10dBm)
- 6mW (7dBm)
- 1mW (0dBm)

For 802.11g:
- 63mW (18dBm)
- 40mW (16dBm)
- 32mW (15dBm)
- 6mW (7dBm)
- 1mW (0dBm)

Receiver Sensitivity
For 802.11a:
- 6Mbps: -87dBm
- 9Mbps: -86dBm
- 11Mbps: -88dBm
- 12Mbps: -85dBm
- 18Mbps: -83dBm
- 24Mbps: -80dBm
- 36Mbps: -76dBm
- 48Mbps: -71dBm
- 54Mbps: -71dBm

For 802.11b:
- 1Mbps: -92dBm
- 2Mbps: -89dBm
- 5.5Mbps: -88dBm
- 11Mbps: -83dBm

For 802.11g:
- 1Mbps: -95dBm
- 2Mbps: -91dBm
- 5.5Mbps: -89dBm
- 6Mbps: -87dBm
- 9Mbps: -85dBm
- 11Mbps: -88dBm
- 12Mbps: -80dBm
- 18Mbps: -80dBm
- 24Mbps: -77dBm
- 36Mbps: -73dBm
- 48Mbps: -72dBm
- 54Mbps: -72dBm

LEDs
- Power
- 10M
- 100M
- 802.11a
- 802.11b/g

Temperature
- Operating: 32ºF to 104ºF (0ºC to 40ºC)
- Storing: -4ºF to 149ºF (-20ºC to 65ºC)

Humidity
- Operating: 10%~90% (non-condensing)
- Storing: 5%~95% (non-condensing)

Certifications
- FCC
- UL

Dimensions
- L = 6.89 inches (175mm)
- W = 4.13 inches (105mm)
- H = 0.79 inches (20mm)

Weight
- 0.44 lbs (200g)

Warranty
- 1 Year

[1] Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11b and 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.
[2] Environmental conditions may adversely affect wireless signal range.

D-Link Systems, Inc. 17595 Mt Herrmann, Fountain Valley CA, 92708-4160 www.dlink.com ©2005 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link, the D-Link logo and *Air*Premier are registered trademarks of D-Link Corporation or its subsidiaries in the United States and other countries. Other trademarks are the property of their respective owners. All references to speed are for comparison purposes only. Product specifications, size and shape are subject to change without notice, and actual product appearance may differ from that depicted herein. Visit www.dlink.com for more details.

D-Link®
Building Networks for People

D-Link
Building Networks for People

DWL-AG132

AirPremier AG

Wireless 108AG USB Adapter

FEATURES

Dualband Wireless Connectivity:
- Up to 108Mbps Using 802.11a/g[1]
- 802.11b Backward Compatible

Convenient USB Connectivity:
- USB 2.0 Ports for Desktops or Notebook PCs
- Backward Compatible to USB 1.1 Ports[2]

Industry Standard Wireless Network Encryption:
- WPA-Personal
- WPA-Enterprise
- WEP (Wired Equivalent Privacy)

Business-class User Authentication:
- 802.1x RADIUS
- EAP-TLS (Extensible Authentication Protocol)
- EAP-TTLS (Extensible Authentication Protocol)

Certifications:
- Wi-Fi 802.11a
- Wi-Fi 802.11b
- Wi-Fi 802.11g

D-Link's *Air*Premier® AG line of 802.11a/g networking products offer a variety dualband wireless connectivity options. Dualband wireless connectivity enables more versatility in network deployment, which can maximize your network investment. D-Link proudly introduces the newest member of the *Air*Premier AG family, the DWL-AG132 Wireless USB Adapter.

The DWL-AG132 is a Wireless USB 2.0 Adapter that adds high-performance 802.11a/g wireless connectivity to your desktop or notebook PC via the convenience of USB. Avoid the hassle of stringing Ethernet cables to your computer or dismantling your desktop PC case to insert a wireless adapter. Simply plug in the DWL-AG132 into an available USB 2.0[2] port and enjoy the freedom of wireless networking.

Powered by D-Link 108AG Technology, this Wireless 108AG USB Adapter is capable of delivering maximum wireless signal rates of up to 108Mbps[1] when used with other *Air*Premier AG devices. Dualband capability ensures that the DWL-AG132 is compatible with virtually all 802.11a/b/g networks and devices.

The DWL-AG132 is designed to connect out of the box with other *Air*Premier AG products making this USB adapter a plug and play solution. An installation wizard make simplifies device discovery and driver configuration. Thereafter, the site survey configuration utility discovers available nearby wireless networks to get you connected quickly. This utility can create detailed connectivity profiles to save and manage your most frequently accessed networks.

For accessing secure networks, this Wireless USB Adapter supports both WPA-Personal and WPA-Enterprise. Now you can utilize EAP-TLS and EAP-TTLS for secure user authentication through an 802.1x RADIUS server. Data over the air is encrypted using either TKIP. Future upgrades to the DWL-AG132 firmware will ensure support for the IEEE 802.11i security specification.

The DWL-AG132 can be used in peer-to-peer mode (ad-hoc) to directly connect to other 802.11a or 802.11b/g devices for direct file sharing, or in client mode (infrastructure) to connect with wireless access points or routers.

The DWL-AG132 features Wi-Fi certification in all three wireless bands, 802.11a, 11b, and 11g, which ensures wireless compatibility and robust data encryption for sensitive data requirements.

Compact in size, this Wireless 108AG USB Adapter is great for travel and is a convenient solution for providing high-performance dualband wireless connectivity to your desktop or notebook PC.

Product Data Sheet

AirPremier AG

DWL-AG132

Wireless 108AG USB Adapter

Specifications

Standards:
- 802.11a
- 802.11b
- 802.11g
- USB 2.0
- USB 1.1

Device Management
- D-Link Wireless Utility

Data Rate[1]
- 802.11a - 108, 54, 48, 36, 24, 18, 12, 9 and 6Mbps
- 802.11g - 108, 54, 48, 36, 24, 18, 12, 9 and 6Mbps
- 802.11b - 11, 5.5, 2 and 1Mbps

Security
- 64/128-bit WEP
- WPA-Personal
- WPA-Enterprise (includes 802.1x)

Wireless Frequency Range
- 5.15GHz – 5.85GHz
- 2.4GHz – 2.497GHz

Wireless Operating Range[3]
- Indoors: Up to 328 feet (100 meters)
- Outdoors: Up to 1,312 feet (400 meters)

Modulation Technology
- Orthogonal Frequency Multiplexing (OFDM)
- Complementary Code
- Direct Sequence Spread Spectrum (DSSS)

Receiver Sensitivity
- 802.11a: -66dBm for 108Mbps @ 10% PER
- 802.11g: -88dBm at 6Mbps @ 10% PER
- 802.11g: -86dBm at 9Mbps @ 10% PER
- 802.11g: -84dBm at 12Mbps @ 10% PER
- 802.11g: -82dBm at 18Mbps @ 10% PER
- 802.11g: -78dBm at 24Mbps @ 10% PER
- 802.11g: -74dBm at 36Mbps @ 10% PER
- 802.11g: -69dBm at 48Mbps @ 10% PER
- 802.11g: -66dBm at 54Mbps @ 10% PER
- 802.11g: -70dBm at 108Mbps @ 10% PER
- 802.11b: -82dBm for 11Mbps @ 8% PER
- 802.11b: -87dBm for 2Mbps @ 8% PER

Wireless Transmit Power
- 11g – +15dBm @ 54 and 48Mbps
- 11g – +16dBm @ 36Mbps
- 11g – +17dBm @ 24, 18, 12, 9 and 6Mbps
- 11b – 16dBm @ 11, 5.5, 2 and 1Mbps

External Antenna Type
- Integrated Antenna

LEDs
- Activity
- Link

Power Consumption
- 472 mA in continuous transmit mode
- 290 mA in continuous receive mode

Temperature
- Operating: 0° C to +40° C
- Non-Operating: -20° C to +75° C

Humidity
- Operating: 20% - 80% (non-condensing)
- Non-operating: 5% to 95% (non-condensing)

Certifications
- FCC
- UL

Dimensions
- L – 3.23in (82mm)
- W – 1.10in (28mm)
- H – 0.47in (12mm)

Weight
- 0.81lbs

Warranty
- 1 Year

[1] Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11b and 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.
[2] Using a USB 1.1 Port will affect device performance.
[3] Environmental conditions may adversely affect wireless signal range.

D-Link Systems, Inc. 17595 Mt Herrmann, Fountain Valley CA, 92708-4160 www.dlink.com ©2004 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link, the D-Link logo and *Air*Premier are registered trademarks of D-Link Corporation or its subsidiaries in the United States and other countries. Other trademarks are the property of their respective owners. All references to speed are for comparison purposes only. Product specifications, size and shape are subject to change without notice, and actual product appearance may differ from that depicted herein. Visit www.dlink.com for more details.

D-Link®
Building Networks for People

WIRELESS INTERNET CAMERA

3G MOBILE VIDEO SUPPORT[1]
View a live camera feed from your compatible 3G mobile phone or PDA

SUPERIOR IMAGE QUALITY
High resolution streaming for detailed viewing locally and remotely

MOTION TRIGGERED RECORDING
Starts recording and sends e-mail alerts upon motion detection

3G MOBILE VIDEO FROM YOUR PHONE AND MORE

The DCS-2120 offers both consumers and small businesses a flexible and convenient way to remotely monitor a home or office in real time from anywhere within a mobile phone's 3G service area. When used in conjunction with the email alert system, mobile users can now view a camera feed without a notebook PC and wireless hotspot. This live video feed can then be accessed through 3G cellular networks by compatible cell phones.[1]

In addition to cellular phone monitoring, the 3GPP/ISMA video format also enables streaming playback on a computer. The camera is also viewable from any Internet Streaming Media Alliance (ISMA) compatible device and offers support for RealPlayer® 10.5 and QuickTime® 6.5 viewing. The DCS-2120 supports resolutions up to 640x480 at up to 30fps using compression rates.

CONVENIENT MANAGEMENT OPTIONS

D-Link's IP surveillance camera management software is included to enhance the functionality of the DCS-2120. Manage and monitor up to sixteen compatible cameras simultaneously with this program. You can also use IP surveillance to archive video straight to a hard drive or network-attached storage devices, playback video, and set up motion detection to trigger video/audio recording or send e-mail alerts. Alternatively, you can access and control the DCS-2120 via the web using Internet Explorer. As you watch remote video obtained by the DCS-2120, you can take snapshots directly from the web browser to a local hard drive, making it ideal for capturing any moment no matter where you are.

ADVANCED RECORDING FEATURES

The DCS-2120 features light sensitivity down to 0.5 lux and is capable of capturing video in rooms with minimal lighting. Low lux sensitivity ensures that the camera's picture quality remains stellar even when lighting conditions change. This, coupled with the camera's 4x digital zoom[2], makes the DCS-2120 a potent surveillance solution. The DCS-2120 is a cost-effective and versatile security solution for your home or business.

D-Link®

LIVE VIDEO MONITORING FROM ANYWHERE

DCS-2120

WHAT THIS PRODUCT DOES

The D-Link DCS-2120 Internet Camera is a full-featured surveillance system that connects to your Ethernet or 802.11g wireless network to provide remote monitoring over the Internet. When monitoring the camera from a computer, you can take snapshots directly from a web browser. The D-Link DCS-2120 Internet Camera is a cost-effective yet powerful security solution for your home office or small-to-medium sized business.

REMOTE MONITORING OPTIONS

The DCS-2120 features 3G mobile video support enabling you to view a live video feed from your camera on a compatible 3G mobile phone or PDA anywhere in your 3G coverage area. The 3G mobile video support expands the functionality of the DCS-2120 allowing you to monitor your remote location without requiring a computer or available Internet connection. IP surveillance software is also included to manage up to 16 cameras simultaneously from your computer, send automated email alerts, and record video to your hard drive when motion is detected.

TECHNICAL SPECIFICATIONS

REMOTE MANAGEMENT
+ Configuration Accessible via a Web Browser
+ Take Snapshots and Save to a Local Hard Drive via a Web Browser

NETWORKING PROTOCOLS
TCP/IP, HTTP, SMTP, FTP, NTP, DNS, DHCP, UPnP™, DDNS, PPPoE

CONNECTIVITY
+ 802.11g Wireless
+ 10/100Mbps Fast Ethernet
+ Auto Negotiation

VIDEO ALGORITHM SUPPORTED
+ 3G Video/ISMA[1]
+ Enhanced Video Compression Using MPEG4 Simple Profile

VIDEO RESOLUTION[2]
+ Up to 30fps at 160x120
+ Up to 30fps at 176x144
+ Up to 30fps at 320x240
+ Up to 30fps at 640x480

AUDIO
+ 16kbps~128kbps (AAC)
+ 4.75kbps~130kbps (GSM-AMR)

CAMERA SPECIFICATION
+ 1/4" CMOS Sensor
+ 0.5 Lux @ F1.4
+ AGC/AWB/AES
+ Electronic Shutter: 1/60~1/15000 sec.
+ Standard Fixed Mount Type Lens 4mm, F2.0
+ 62˚ Field of View

SECURITY
+ Administrator and User Group Protected
+ Password Authentication

IP SURVEILLANCE SOFTWARE
+ Remotely Manage and Control up to 16 DCS-2120 Internet Cameras
+ View Up to 16 Cameras on one screen
+ Supports all Management Functions Provided in Web Interface
+ Scheduled Motion Triggered, or Manual Recording Options

VIEWING SYSTEM REQUIREMENT PROTOCOL
ActiveX

BROWSER
Internet Explorer v6

LEDS
Two-Color LED

POWER
+ External Power Supply
+ 5V DC 2.0A
+ Power Consumption 5.5W

DIMENSIONS
4.5" (L) x 3.125" (W) x 1.625" (H)

WARRANTY
1-Year[3]

[1] 3G phone must be equipped with 3G video playback such as RealPlayer® or PacketVideo for Symbian or PocketPC.
[2] 4X digital zoom enlarges an image by magnifying the pixels in a selected portion of the image by 4 times.
[3] 1-Year Warranty available only in the U.S.A. & Canada.
[4] Latest software and documentation are available at http://support.dlink.com.

Use of audio or video equipment for recording the image or voice of a person without their knowledge and consent is prohibited in certain states or jurisdictions. Nothing herein represents a warranty or representation that the D-Link product provided herein is suitable for the end-user's intended use under the applicable laws of his or her state. D-Link disclaims any liability whatsoever for any end-user use of the D-Link product which fails to comply with applicable state, local or federal laws.

All references to speed are for comparison purposes only. Product specifications, size and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.

SECURITY

MINIMUM SYSTEM REQUIREMENTS
Computer with:
- 1.3 GHz Processor
- 256MB Memory
- Windows® XP SP2 or Windows 2000 SP4
- Internet Explorer v6

Multiple Camera Operation Requires PC with:
- 2.4 GHz Processor
- 512MB RAM
- 32MB Video Card

PACKAGE CONTENTS
- Wireless Internet Camera
- Detachable Antenna
- CAT5 Ethernet Cable
- Power Adapter
- Mounting Kit
- Quick Installation Guide
- CD-ROM[4] with
  - Software
  - Product Documentation
  - Special Offers

D-Link Systems, Inc. 17595 Mt. Herrmann Street Fountain Valley CA 92708 www.dlink.com
©2006 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link and the D-Link logo are registered trademarks of D-Link Corporation or its subsidiaries in the United States and other countries. Other trademarks or registered trademarks are the property of their respective owners. Visit www.dlink.com for more details.

REFERENCIAS BIBLIOGRÁFICAS

- RANDALL K. Nichols, PANOS C. Lekkas, *Seguridad para comunicaciones inalámbricas*, Mc. Graw-Hill, USA, 2003.

- CABALLAR, Falcon, *WI-FI. Cómo construir una red inalámbrica,* segunda edición, 2004.

- ANDREU, PELLEJERO, LESTA, *Redes WLAN. Fundamentos y aplicaciones de seguridad en redes wlan,* Marcombo ediciones tecnicas, Barcelona, 2006.

- Tipos de redes inalámbricas, http://www.monografias.com.

- Protocolos de seguridad en redes inalámbricas, http://www.saulo.net.

- Calificación de equipos inalámbricos, http://www.ecoustics.com.

- Selección de equipos y hojas técnicas, http://www.dlink.com.

- Seguridad RADIUS, http://www.authenter.com.

- Redes inalámbricas de área local, estándares IEEE servidores Radius, http://es.wikipedia.org.

- Revisión de productos inalámbricos, http://www.belkin.com.

- Revisión de productos inalámbricos, http://www.linksys.com.

Sangolquí,_____

Elaborado por:

_____

C. ANDRÉS AMAYA MANTILLA

Coordinador de La Carrera

Secretario Académico

_____

ING. GONZALO OLMEDO

_____

AB. JORGE CARVAJAL